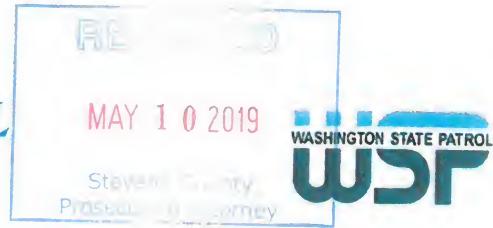


WASHINGTON STATE PATROL
CRIMINAL INVESTIGATION DIVISION
Investigative Report



FILE TITLE Attempted Theft 1 st degree	DETECTIVE Larry McGill #770	CASE NUMBER SCSO# 1903342
SUBJECT James R. Bolton		OTHER CASE NUMBER WSP# 04-19-009175

SYNOPSIS:

On April 16, 2019, Stevens County Sheriff's Office (SCSO) requested the assistance of the Washington State Patrol (WSP) to conduct an infotainment acquisition of a vehicle in a criminal investigation. WSP Detective Larry McGill, a certified examiner for Berla iVe infotainment system, performed the acquisition.^{1,2}

DETAILS:

On April 16, 2019, McGill received a phone call from SCSO Detective Frizzell inquiring about him conducting an infotainment acquisition from a vehicle in a criminal investigation. Frizzell provided McGill with a description of the vehicle to verify if the vehicle and system were supported.

Vehicle Description:

2013 Ford Edge
WA license: BDE3849
VIN: 2FMDK4JC9DBB31410
Registered Owner: James Bolton



Image 1: 2013 Ford Edge, VIN: 2FMDK4JC9DBB31410.

Based on the VIN, the vehicle was considered supported by the Berla iVe system. Berla iVe indicated the vehicle may be equipped with either a SYNC Gen1 or a SYNC Gen2 system. Frizzell provided McGill with a photograph of the center stack of the dash area as well as the

1 Berla iVe is a vehicle forensics solution for identifying, acquiring and analyzing critical data from vehicle systems while conducting an investigation. Berla iVe uncovers critical information stored within vehicle systems and can help determine what happened, where it occurred and who was involved.

2 WSP Detective McGill successfully completed Berla's Vehicle System Forensics and iVe Certification course in April 2018.

Page 1 of 5

Officer's Signature

Date 5-8-19

Peer Reviewer's Signature

Date 5/8/19

Supervisor's Signature

Date 5/8/19

RECEIVED
MAY 09 2019
Sheriff Records
Stevens Co. Sheriff's Office

263

steering wheel button controls. By the photographs provided, McGill was able to confirm the system was a SYNC Gen1 as there was no touch screen and there was a push-to-talk button on the steering wheel.

The potential data available in a SYNC Gen1 module was listed:

- Connections
 - Bluetooth
 - Unique identifiers
- Devices
 - Phones
 - Unique identifiers
 - Contacts
 - Call logs
- Events
 - Odometer Reading
 - Power
 - Start/Stop Log
- System metadata

McGill advised Frizzell of this potential information and provided him some recommended language to use in a search warrant to describe the infotainment system. McGill also advised Frizzell there are 5 versions of SYNC Gen1 and depending on which version, it could take either 12.5 hours or 40 hours to complete the acquisition. To determine which version, the module would need to be removed and to visually inspect the circuit board inside.

Frizzell advised he would move forward with the search warrant and planned to meet at the SCSO on April 17th at 9:00 a.m.

McGill requested WSP Detective Ben McBride to assist with the module removal.

On April 17, 2019, McGill and McBride contacted Frizzell at the SCSO in Colville. Frizzell provided McGill a copy of the signed search warrant for the Ford, which included an image of the vehicle's infotainment system.

At 9:33 a.m., McGill, McBride and Frizzell contacted the SCSO property/evidence facility where the vehicle was stored inside. The vehicle was sealed on all seams with evidence tape. McGill took exterior and interior photographs of the vehicle.



Image 2: Interior of 2013 Ford Edge with Sync Gen 1 system.

McGill followed the module removal instructions for a Ford Edge provided by Berla. According to the instructions, the module was located at the rear of the center console, just behind the rear vent cover. However, the module was not located behind this cover. McGill contacted Berla support and learned the alternate location for the module was under the center console just behind the gear shift. Berla did not have specific instructions for the Ford Edge, but provided instructions for a similar vehicle.



Image 3: Rear vent cover of center console.

McGill photographed the process of disassembly for documentation and for future use in other module removals in a Ford Edge.³

During the removal process, McGill observed blueish dye in the seams of the plastic panels. McGill advised Frizzell of this his inspection.

At approximately, 11:30 a.m., the module was removed from the vehicle and provided to Frizzell. McGill confirmed the SYNC Gen1 module by the label on the case.



Image 4: SYNC Gen1 module from Ford Edge.



Image 5: Close-up view of label from module.

³ See 2013 Ford Edge SEL AWD Instructions created by McGill.

Once Frizzell logged the module as evidence, he signed it out to McGill for further analysis. McGill transported the module to the WSP Spokane district office to complete the acquisition.

At 3:30 p.m., McGill opened the module case, inspected the circuit board and confirmed the module as a SYNC Gen1 Version 3.

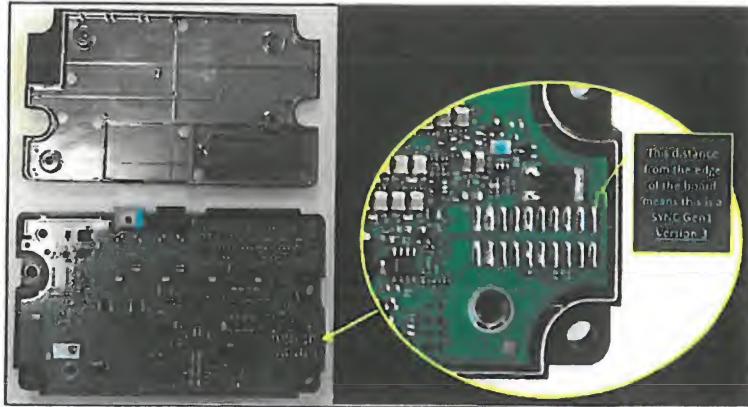


Image 6: Sync Gen1 Version 3 module.

McGill advised Frizzell the imaging process would take approximately 12.5 hours. McGill verified his computer had the latest operating version of Berla iVe software, V. 2.3.0. McGill connected the required hardware and started the acquisition at approximately 4:00 p.m. and secured the equipment in the office to let the program run overnight.

On April 18, 2019, at 6:00 a.m., McGill returned to the office and found the acquisition had completed successfully without any errors.

McGill created a case report of all data using the Berla iVe software to provide to Frizzell for his investigation.

Upon review of the information, the vehicle was originally from Canada. The system reported on the following content.⁴

- Connections: 5
 - Bluetooth: 1
 - USB: 4
- Devices: 5
 - No “Device Name” listed (Unique Number: 04F7E492C3CD) – Bluetooth
 - Contacts: 1644 (*appeared to be mostly Canadian numbers*)
 - Call Logs: 84 (*no specific time stamps listed*)
 - iPhone – USB
 - Media Files: 1
 - Keith’s iPad – USB
 - Media Files: 174
 - SM-G920W8 – USB
 - Media Files: 5
 - Syd the iPhone 4S – USB
 - Media Files: 358

⁴ See iVe Case Report for further details.

- Events: 64
 - System Log: 40
 - Power: 24

There was no data with timestamps to generate a timeline. Timeline items must include calls, events, or tracks with a valid date.

At 10:20 a.m., McGill and McBride returned to the SCSO to meet with Frizzell. McGill provided Frizzell with the iVe Case Report generated earlier and explained to him on how to search the document. McGill, McBride and Frizzell returned to the SCSO property/evidence facility and connected the module back into the vehicle and reassembled the interior.

At 12:31 p.m., the installation was completed.

End of report.

2013 Ford Edge SEL AWD
SYNC Gen 1 Version 3
by McGill, Larry (WSP)

Tools Required

- Berla trim tools
- Nut driver
- $\frac{1}{4}$ " Drive socket wrench with extension
- $\frac{1}{4}$ " Drive 7mm, 8mm, 10mm sockets
- T20 Torx bit
- Long pry tool/bar



270

MF.D. BY FORD MOTOR CO.

DATE: 11/12

GVWR/PNBV: 2531 KG (5580 LB)

FRONT GAWR/PNBE AV / REAR: GAWR/ PNBE AR
1329 KG (2930 LB) 1207 KG (2660 LB)

WITH / AVEC TIRES/PNEUS

P245/60R18 104H

P245/60R18 104H

18x8.0J

RIMS/JANTES 18x8.0J



AI/A kPa/PSI/IPC 240/35

COLD/A FROID

240/35

/JUMELEES

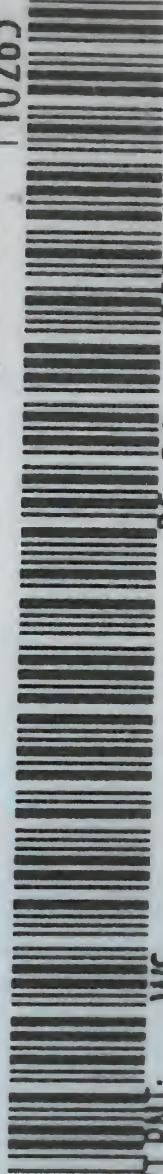
VIN: 2FMDK4JC9DBB31410

TYPE: MPV/VTUM

COMPLIES: ICES/NMB-002

F0194

T0285



EXT PNT:

WS

RC: B6

DSO:

WB INT TR TP/PS R AXLE TR SPR

111 FL

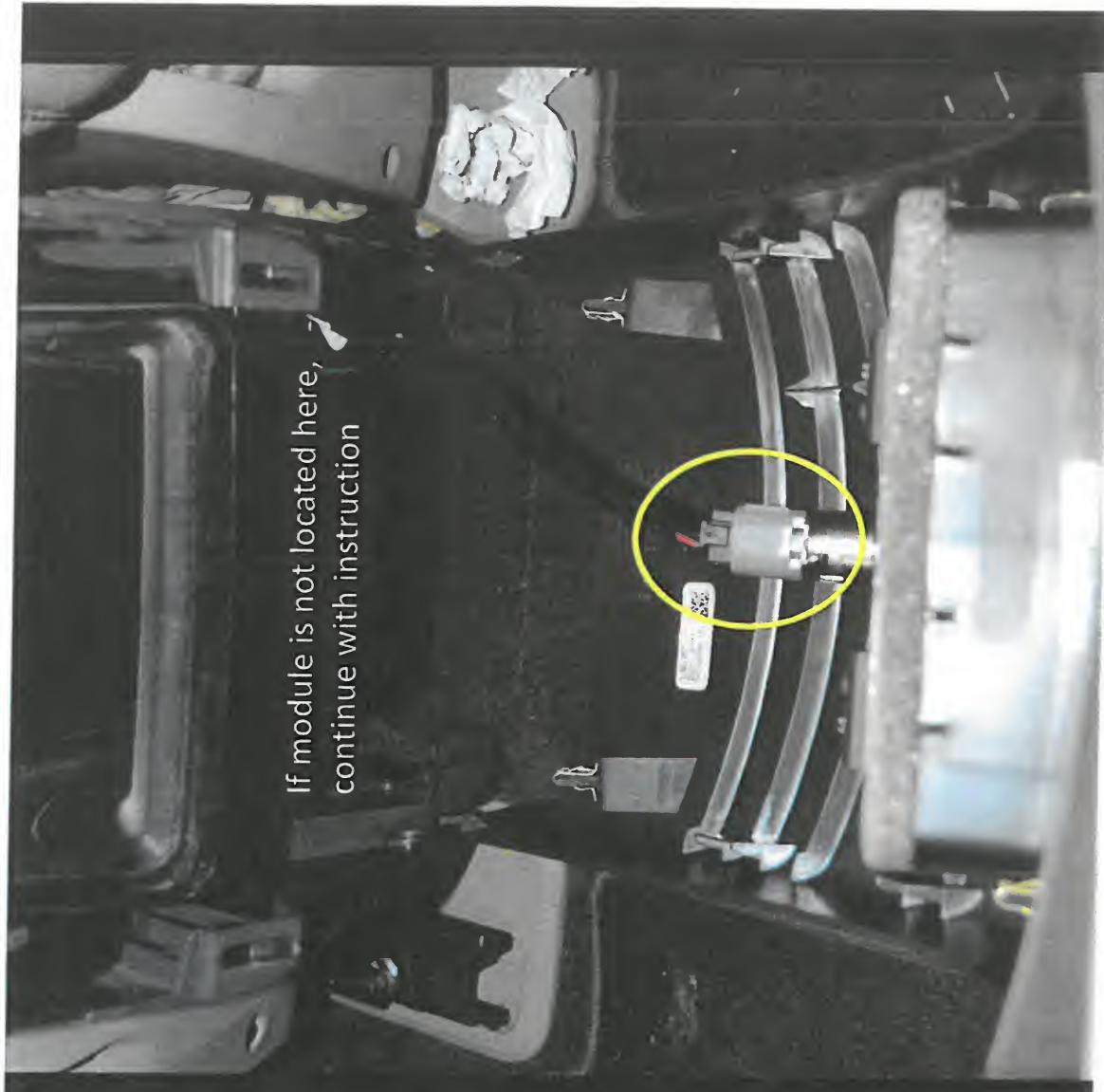
Z 3E J BBBB

UUT ▽5USA-1520472-BA

27

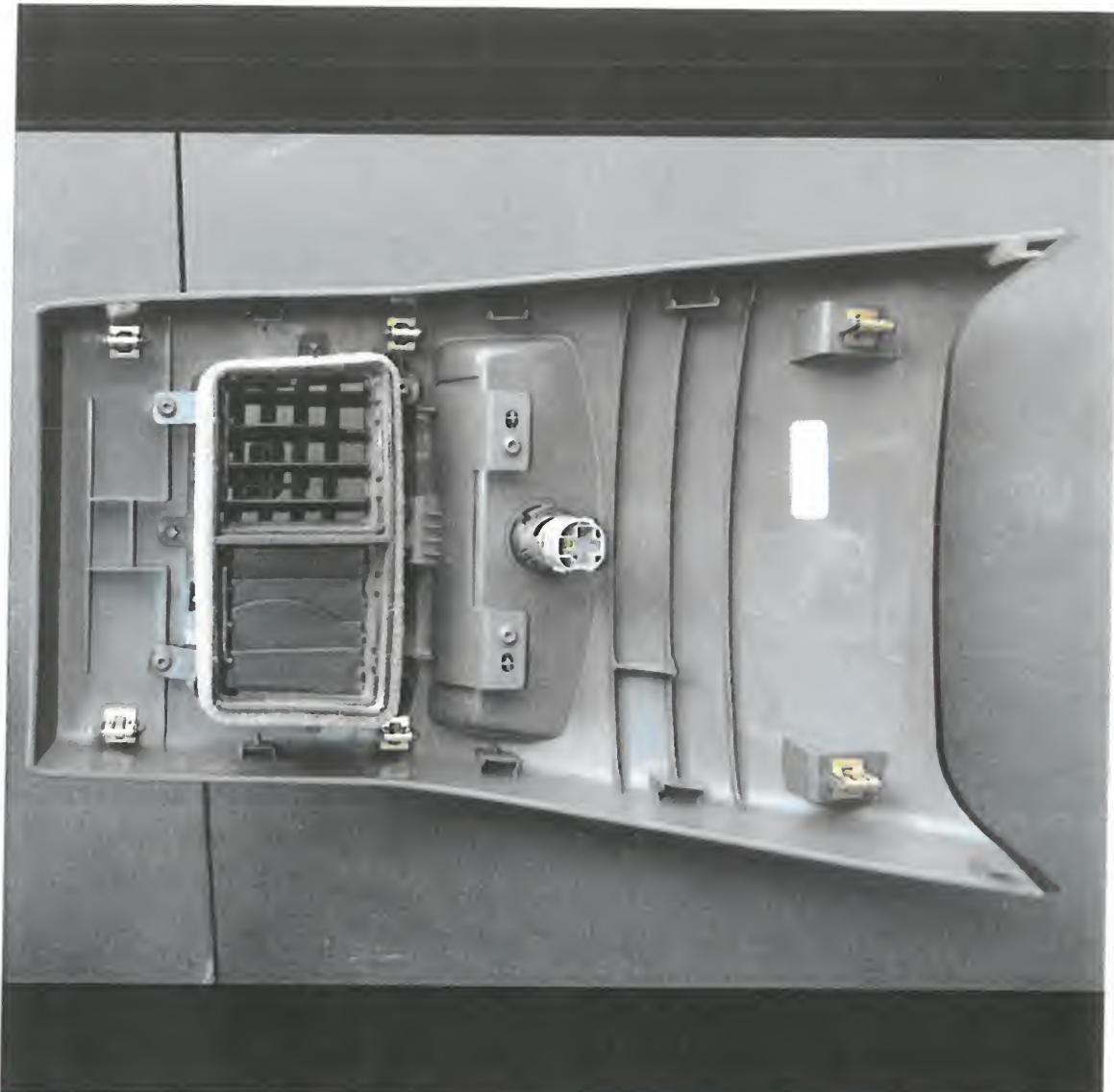


272



If module is not located here,
continue with instruction





274



Passenger's Side



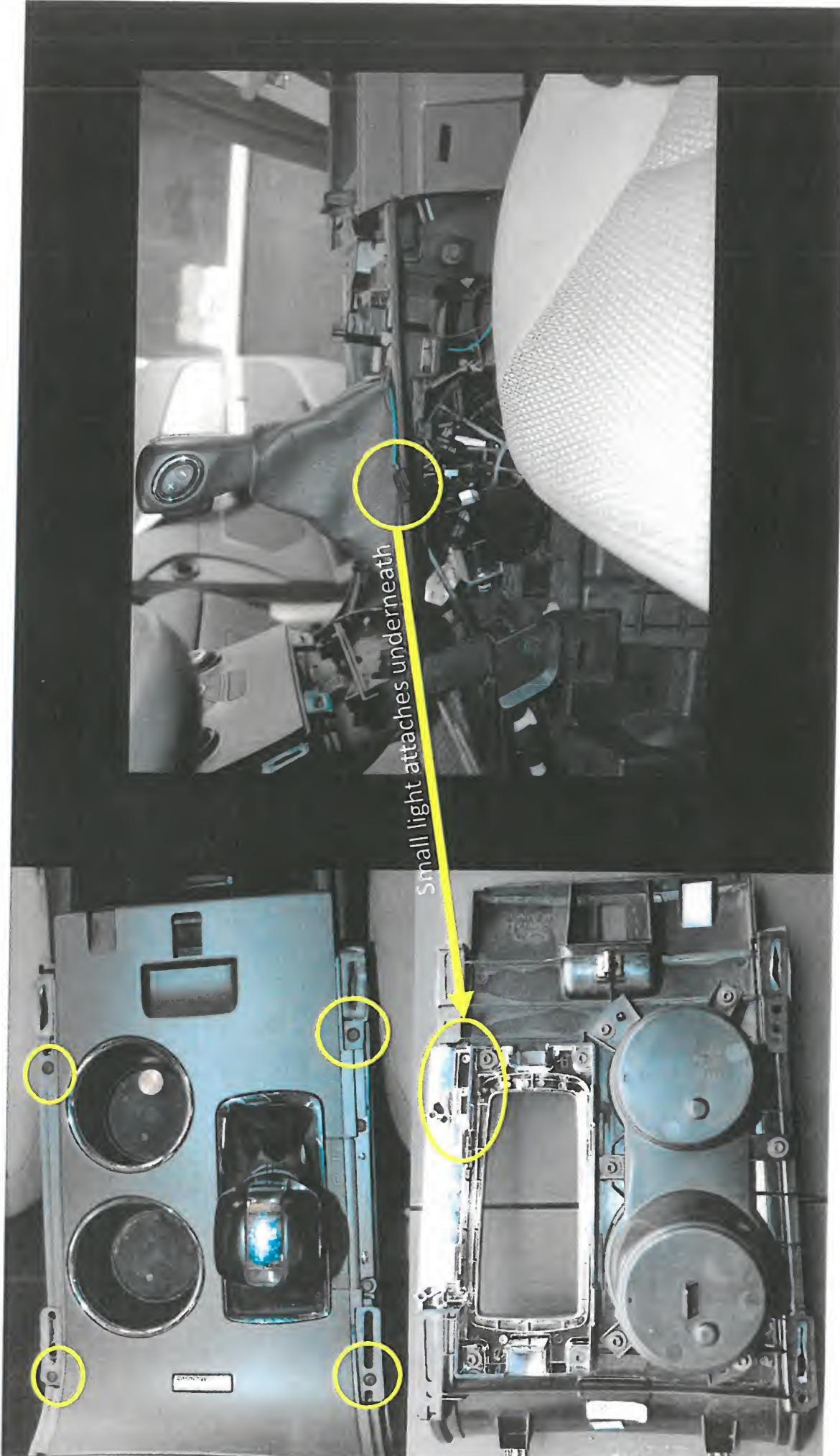
Driver's Side



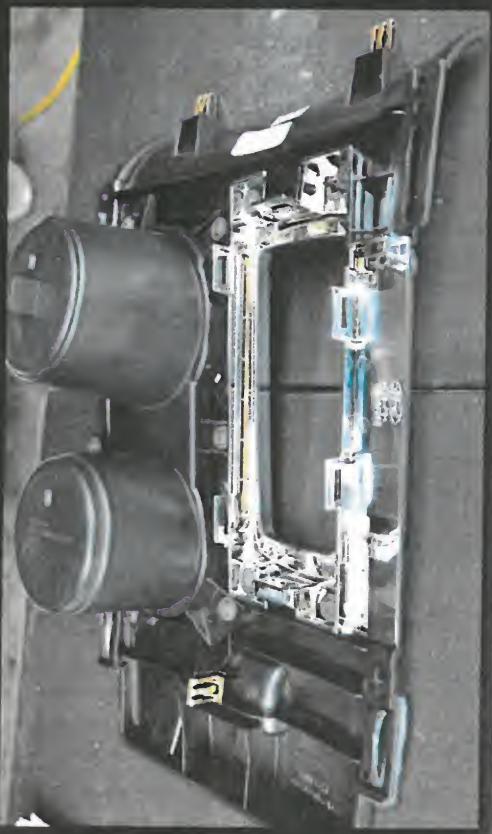
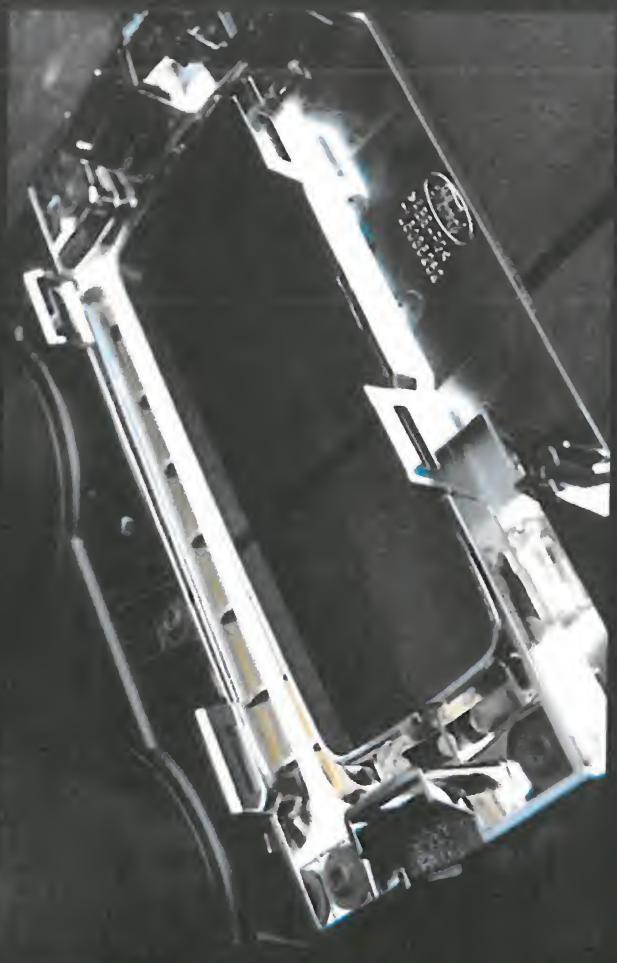
276



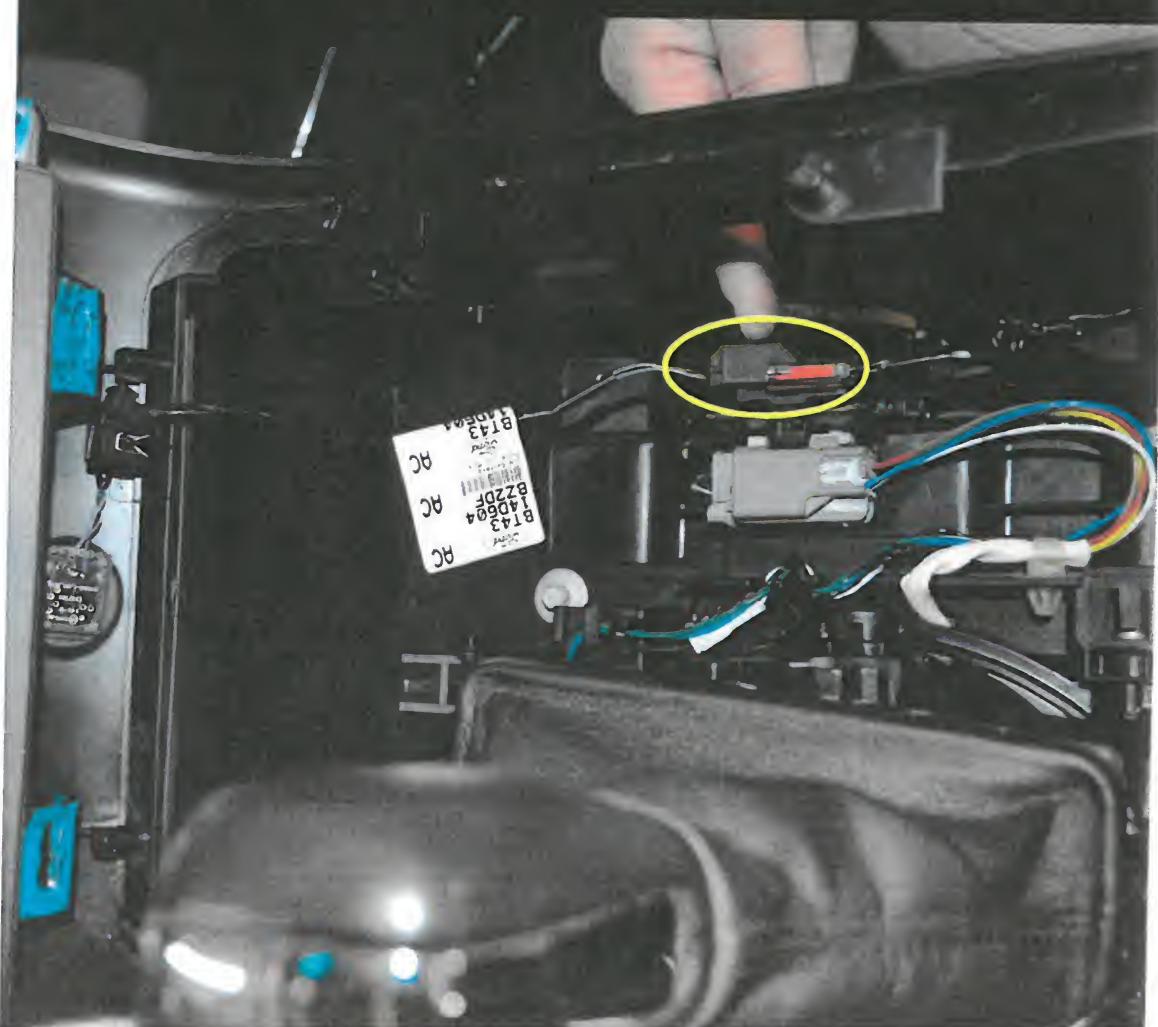


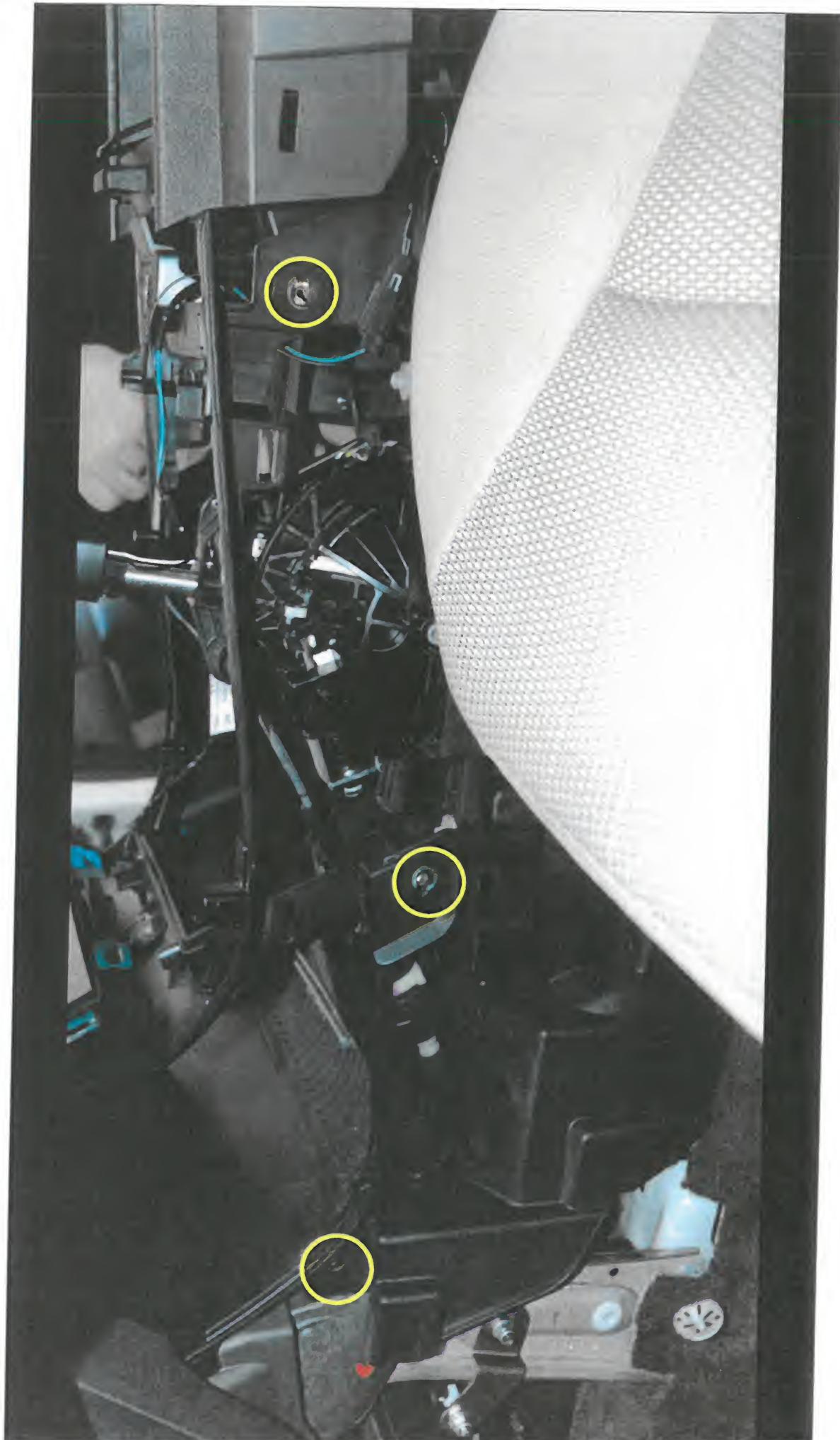


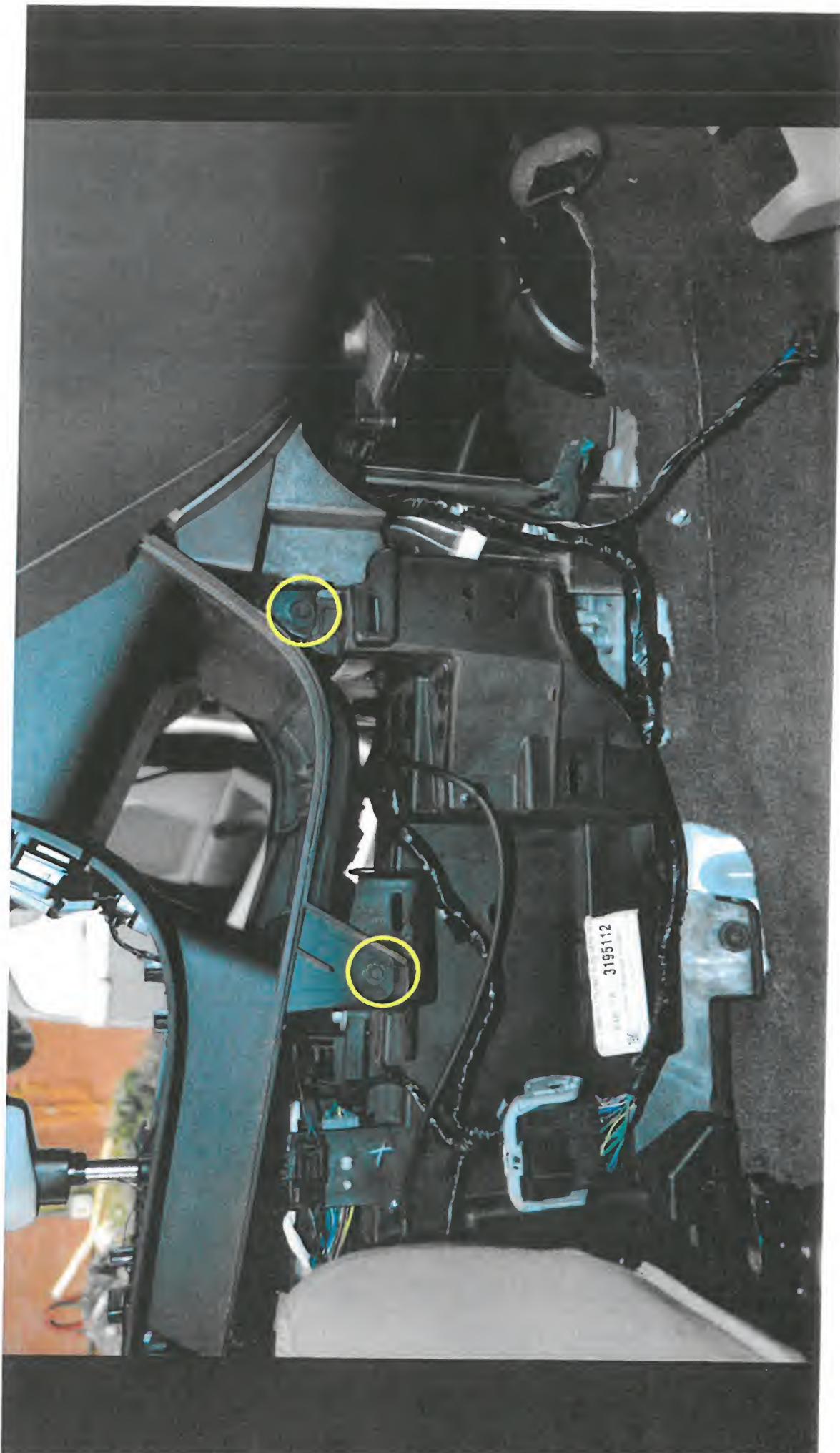
Shifter boot tabs snap underneath the shifter plate.
The forward one slips into the slot.

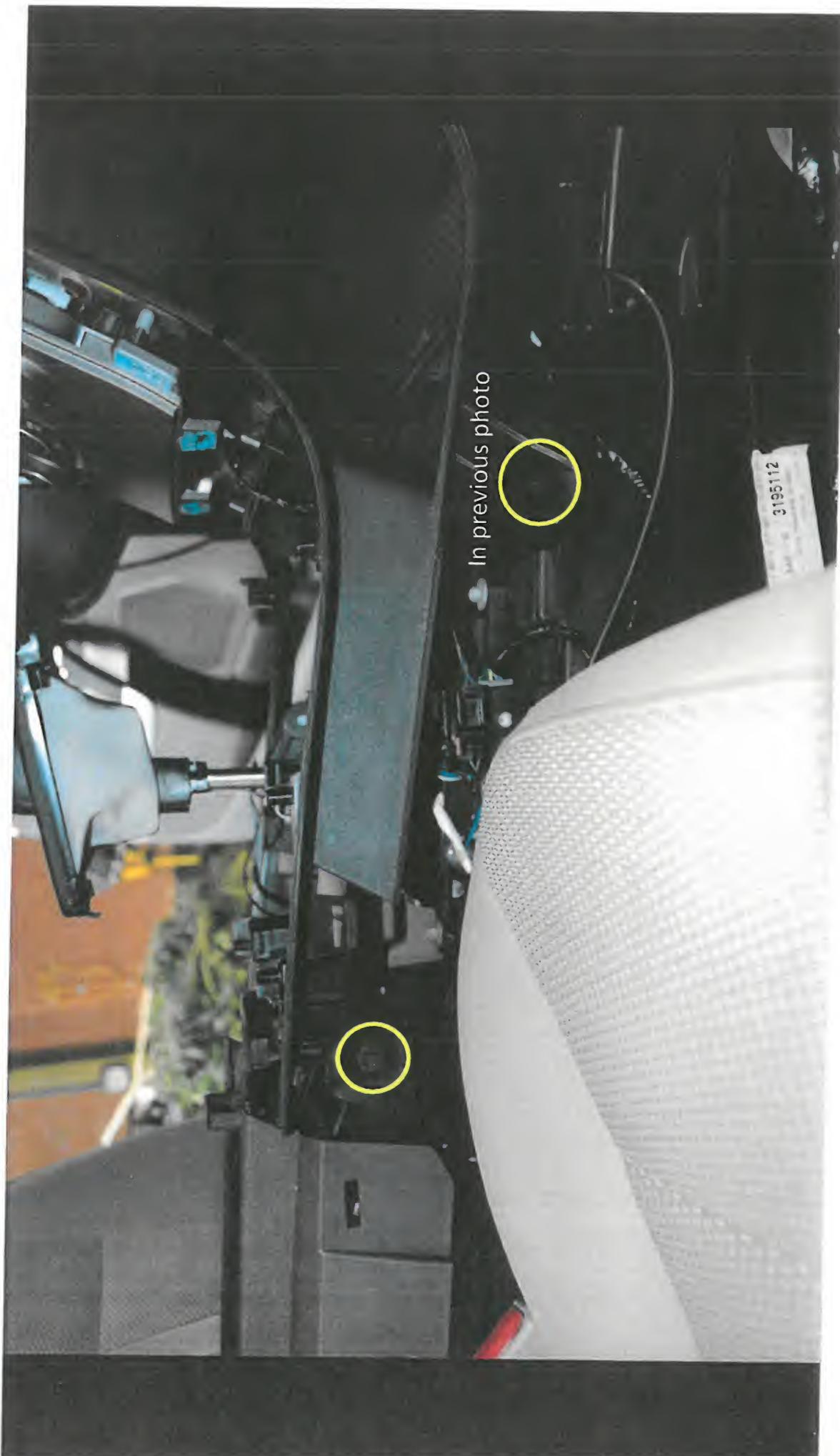


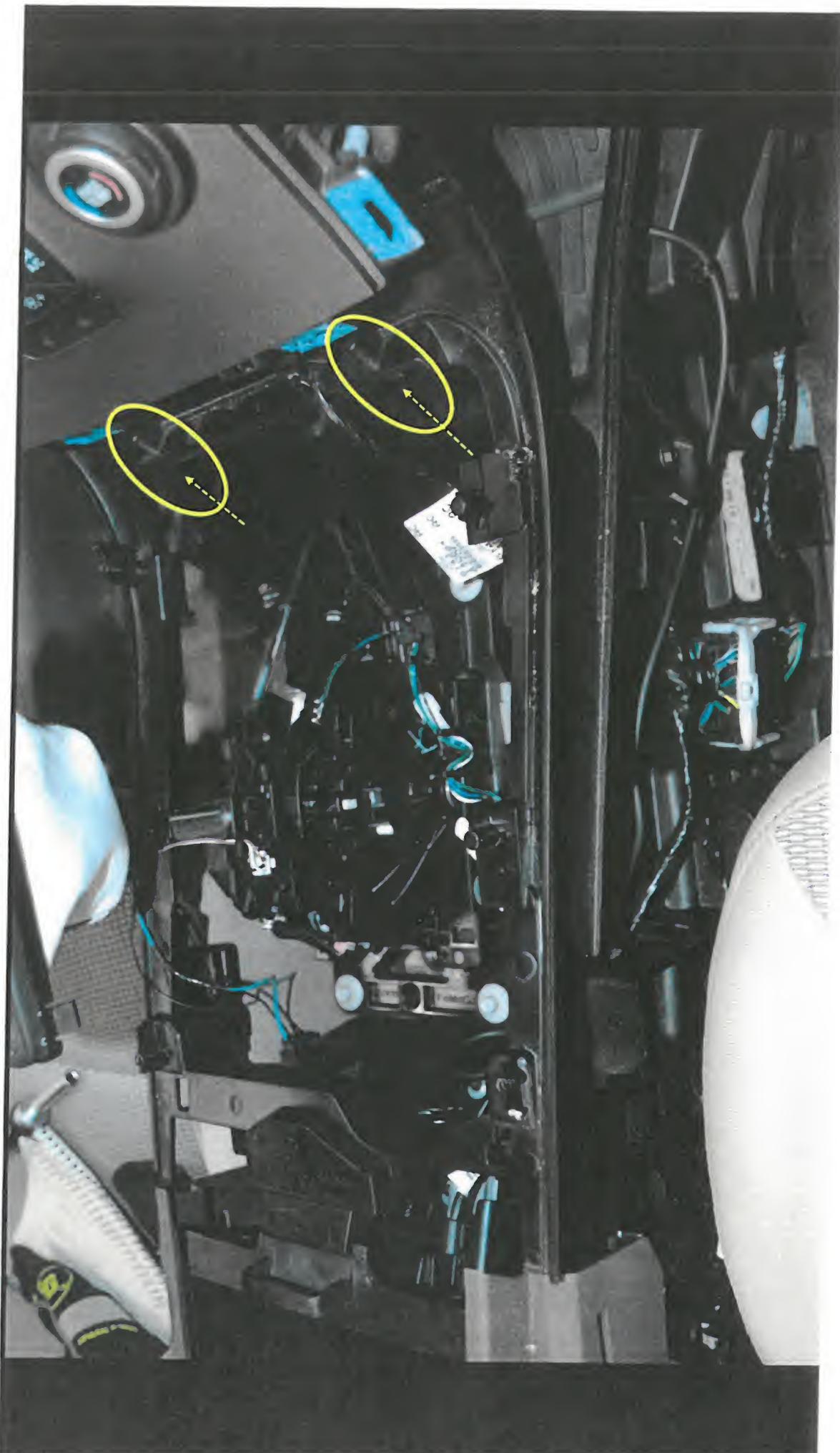
Unplug the low light sensor.









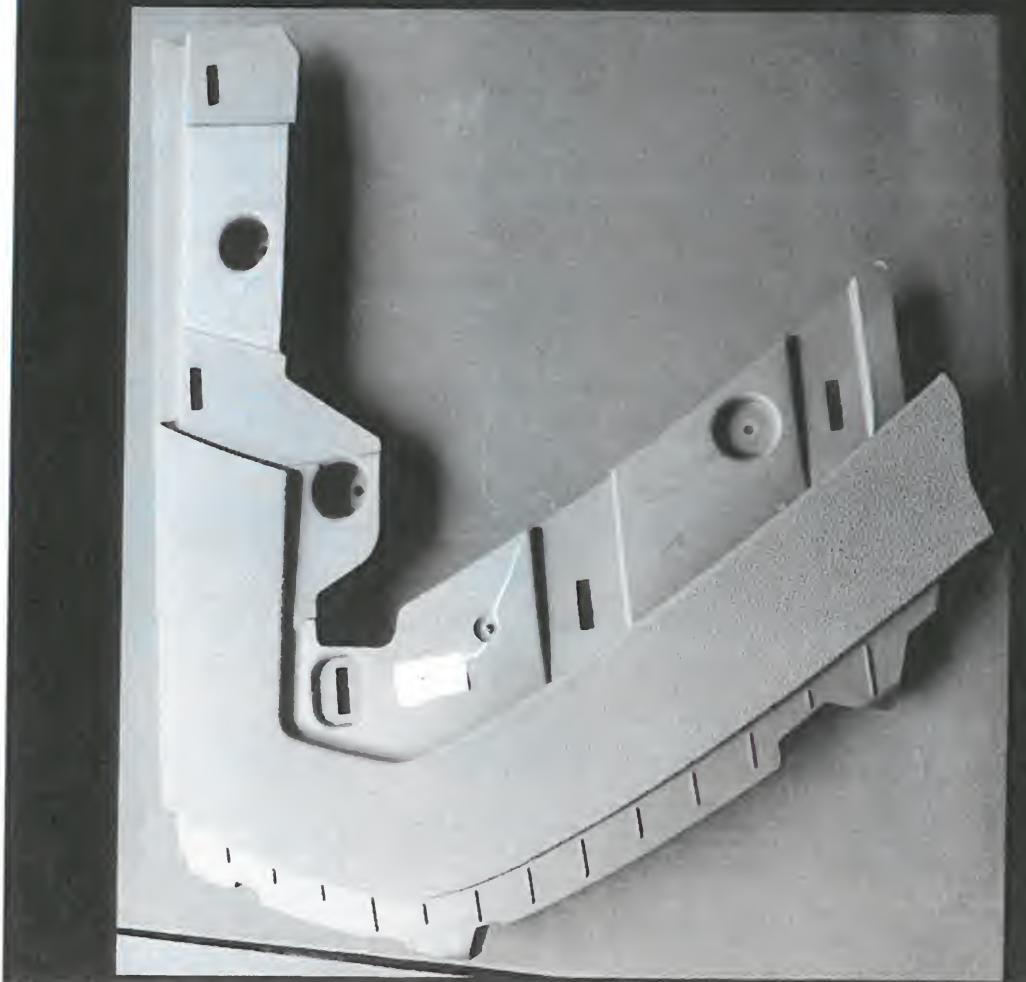
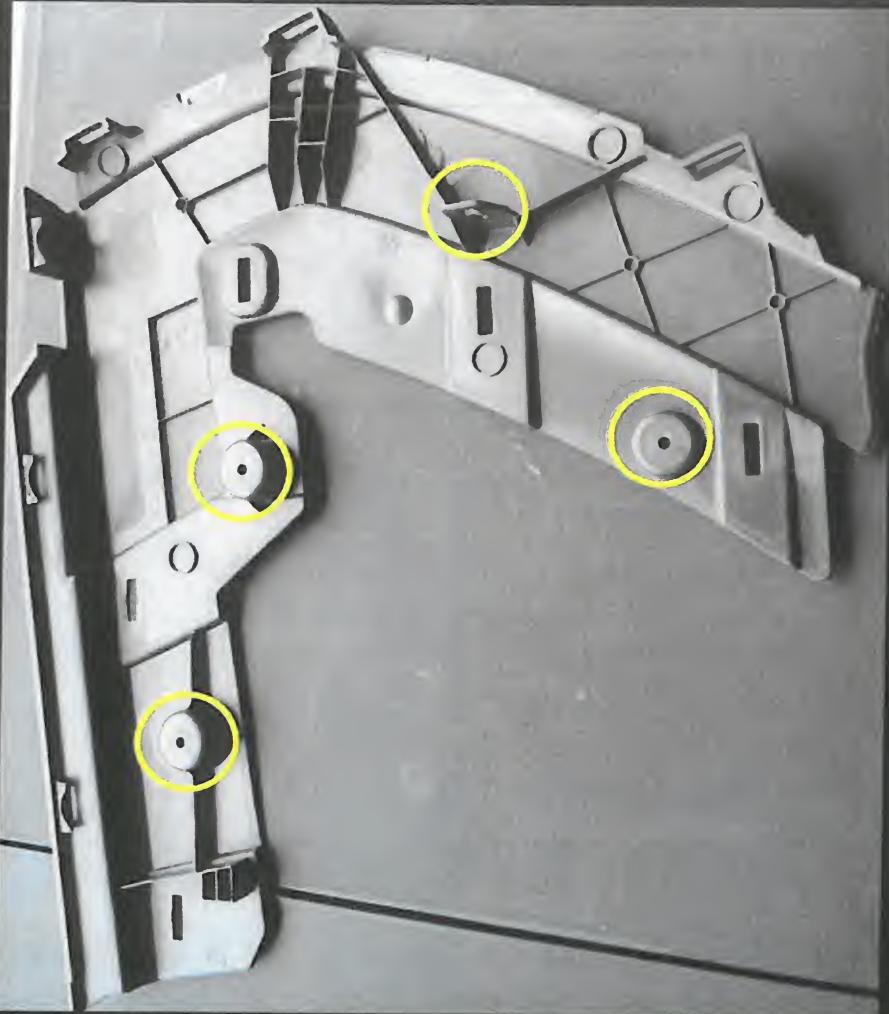




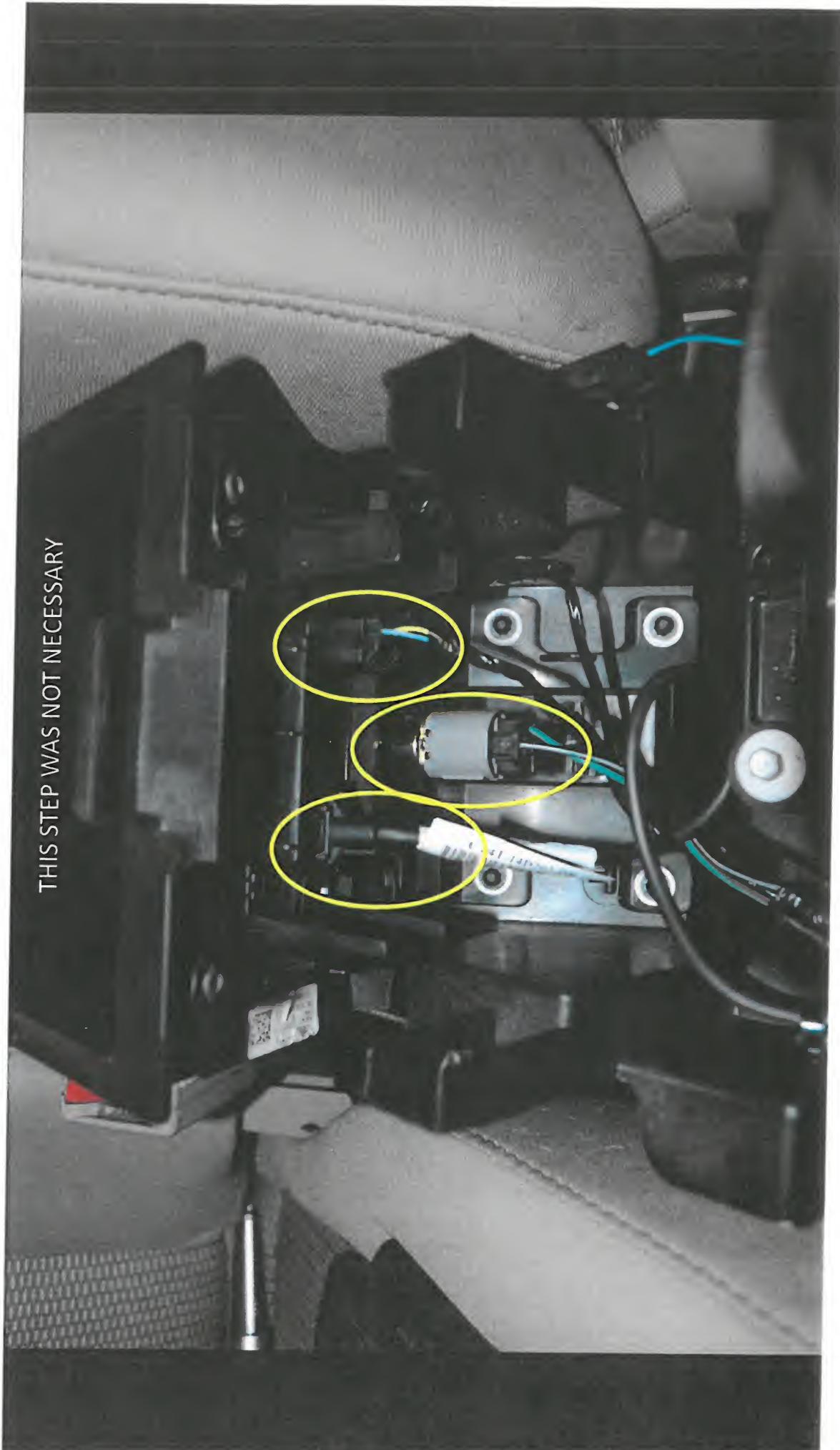
286

Repeat on driver's side



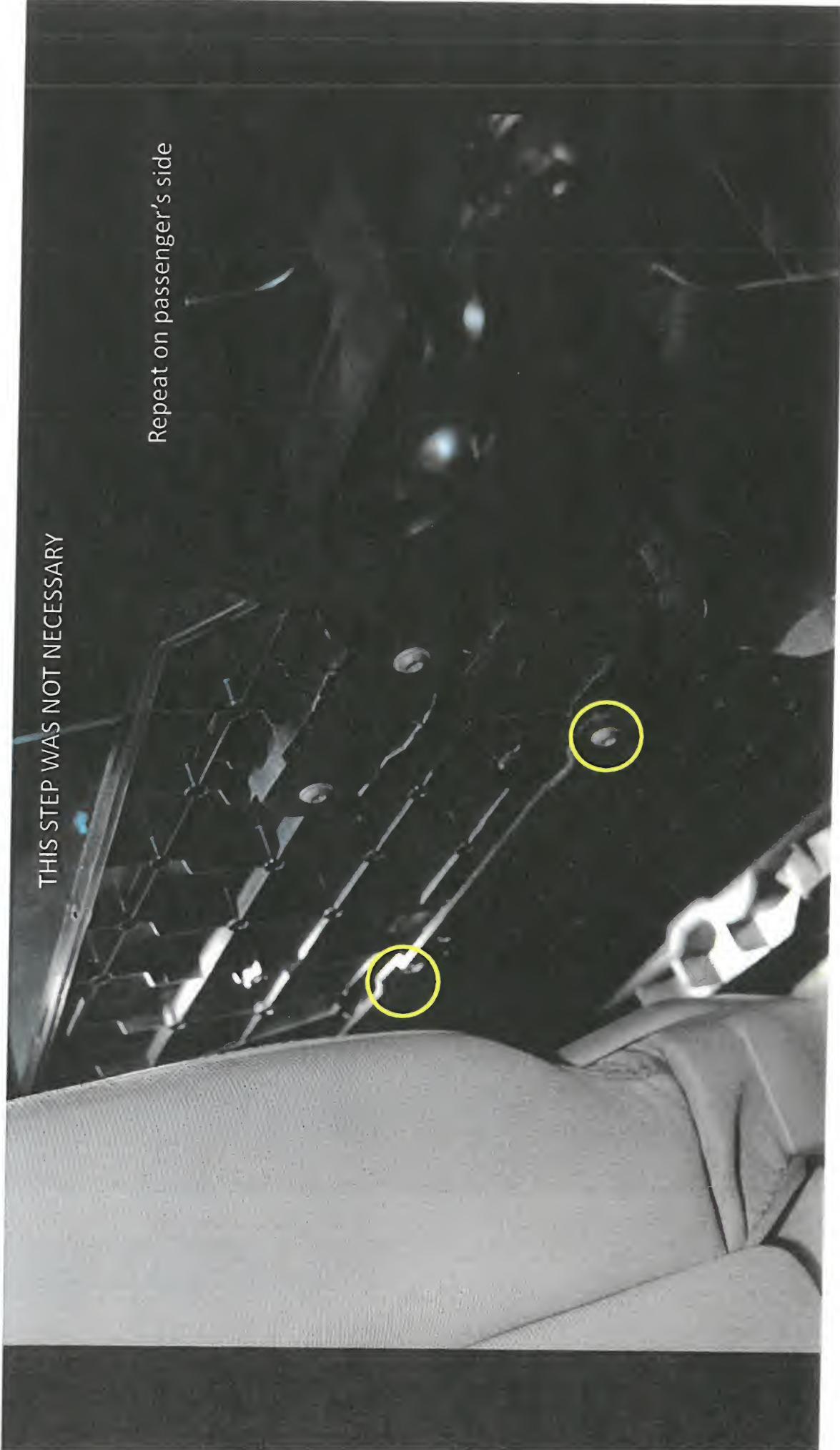


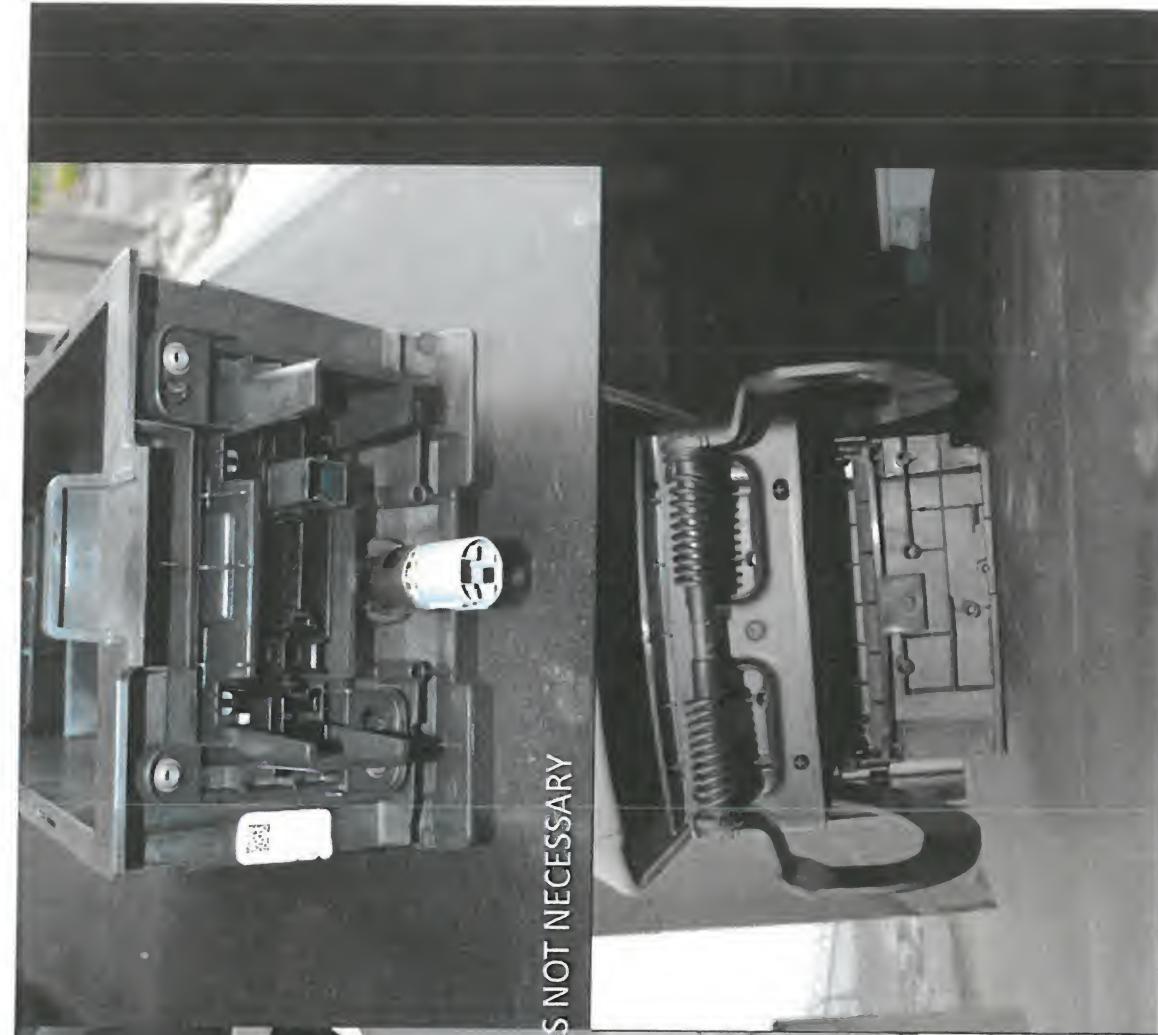
THIS STEP WAS NOT NECESSARY



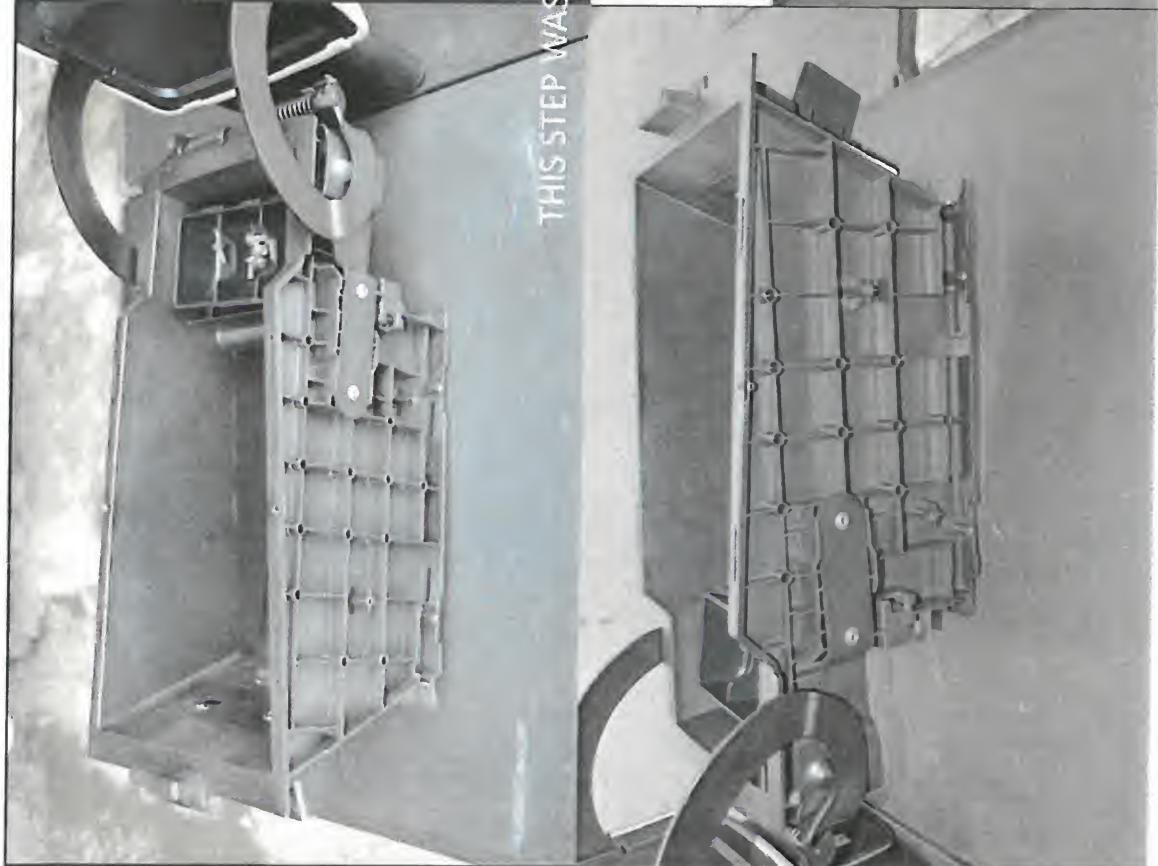
THIS STEP WAS NOT NECESSARY

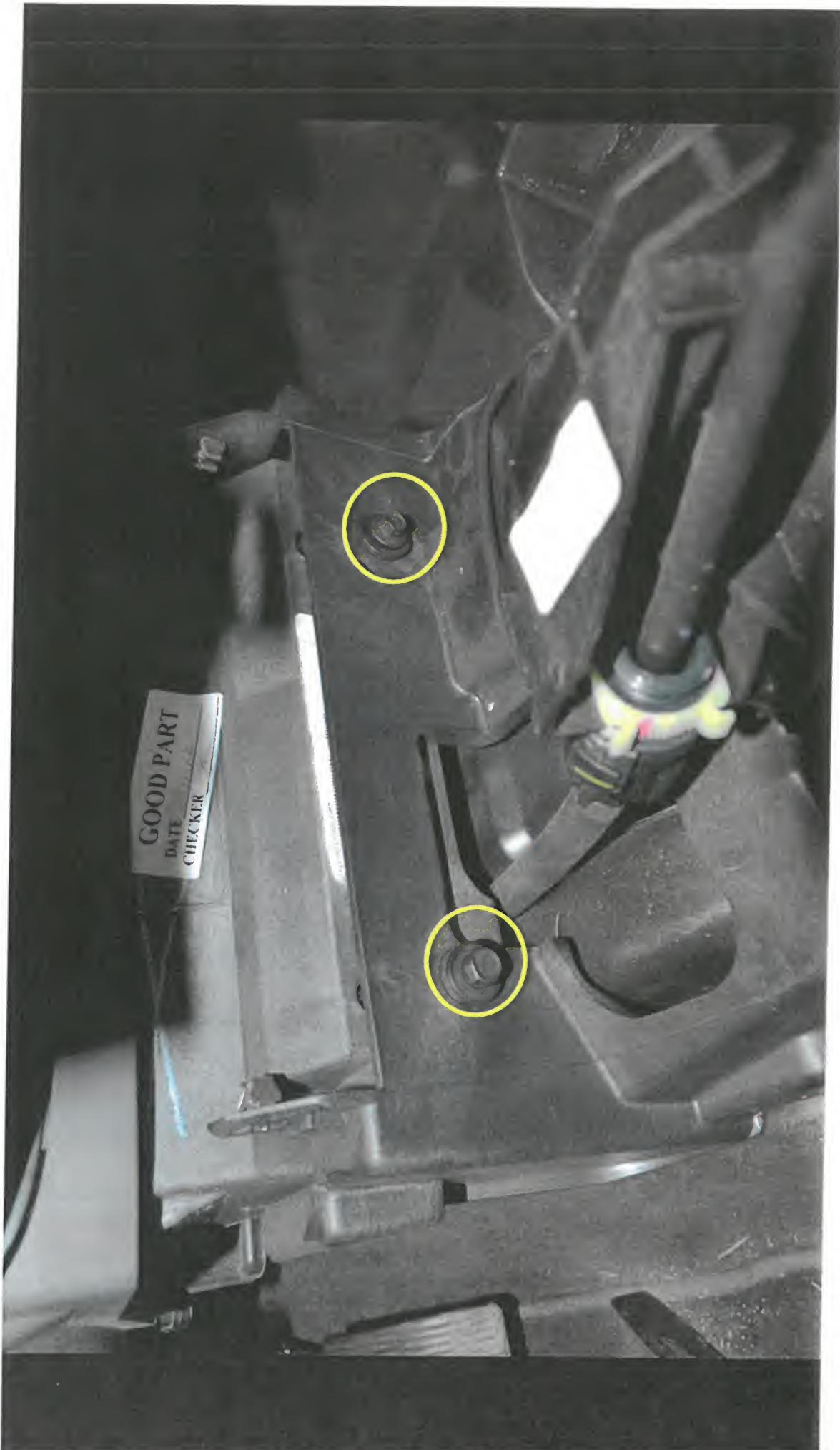
Repeat on passenger's side

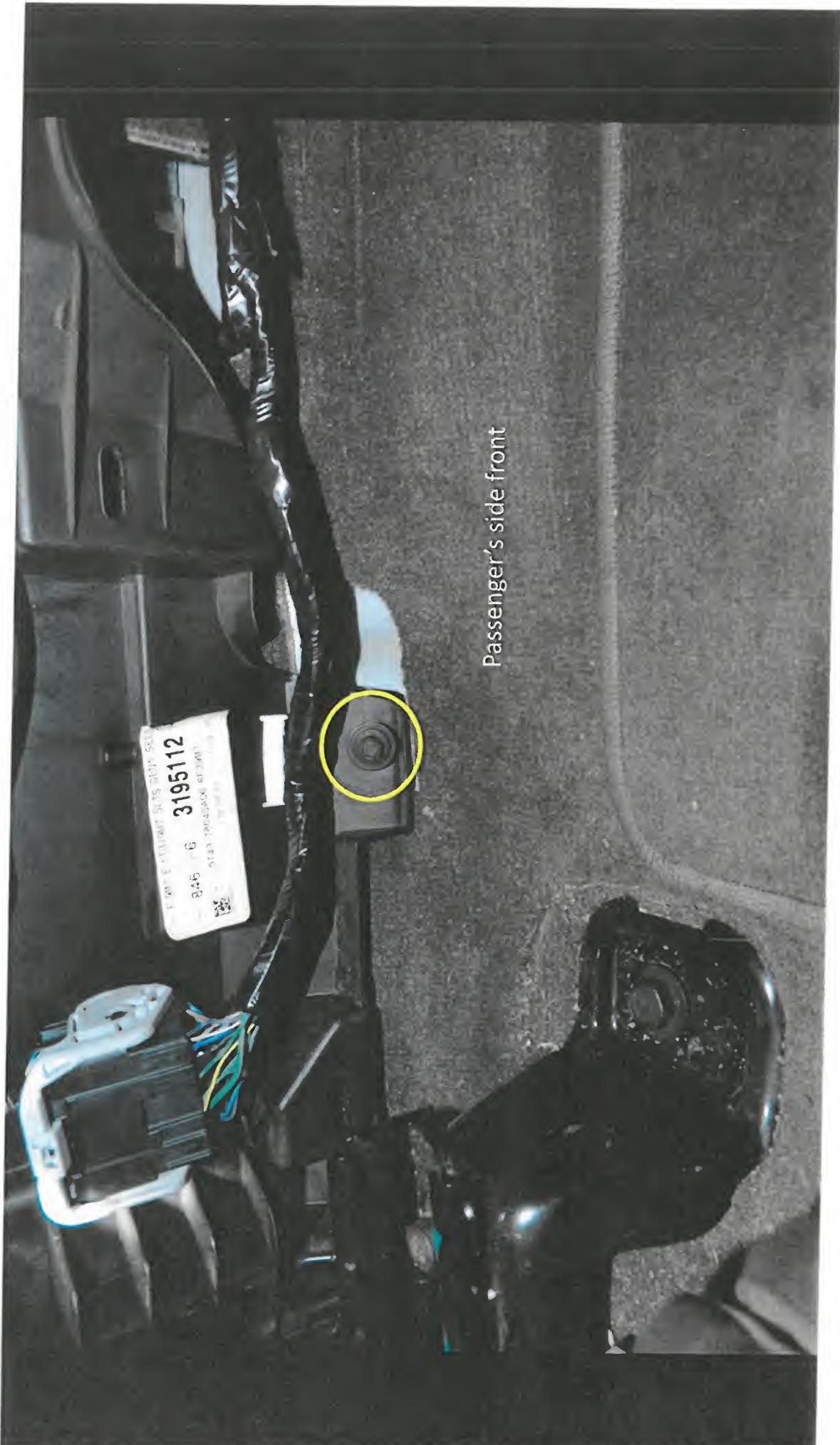




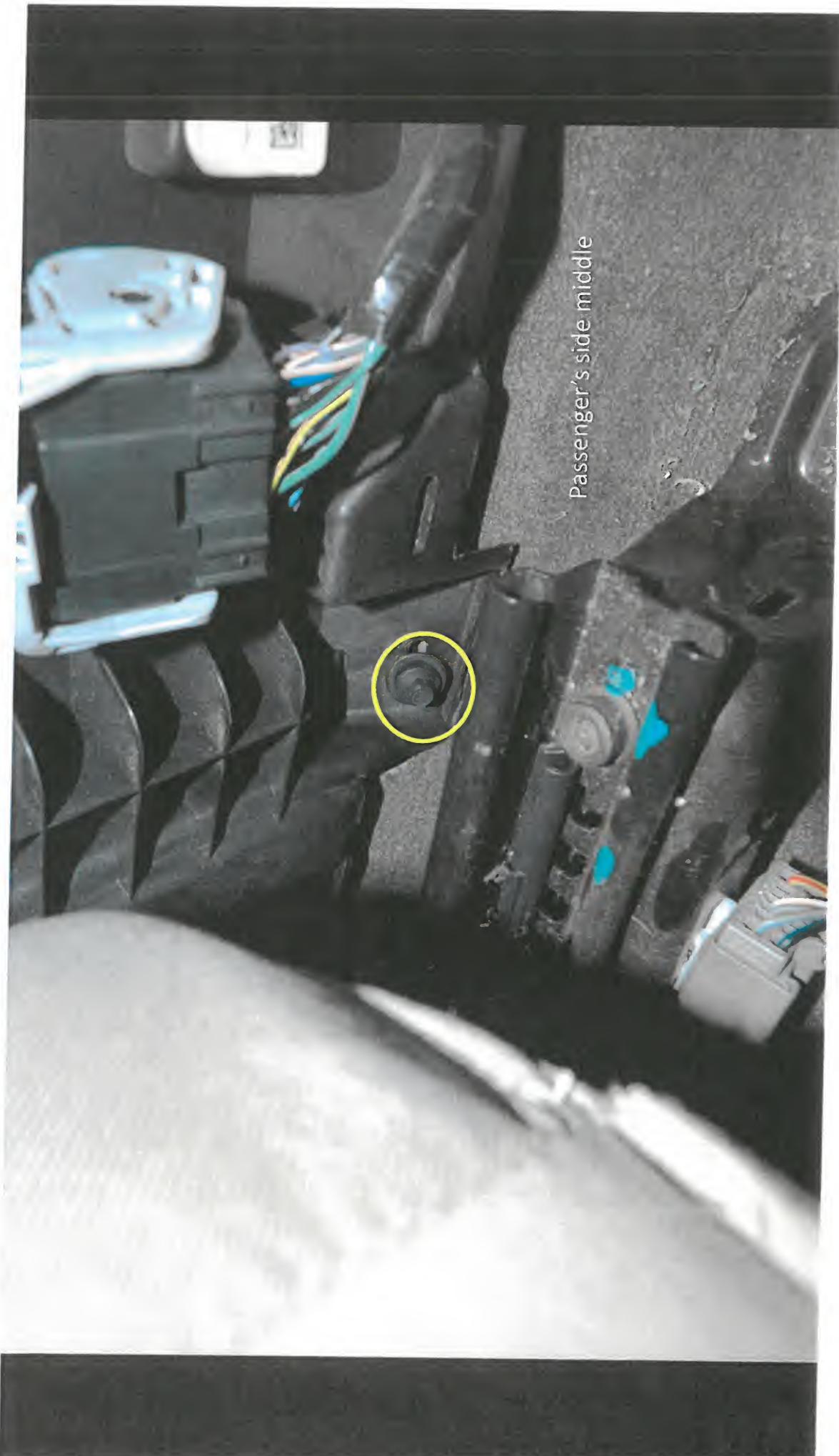
THIS STEP WAS NOT NECESSARY



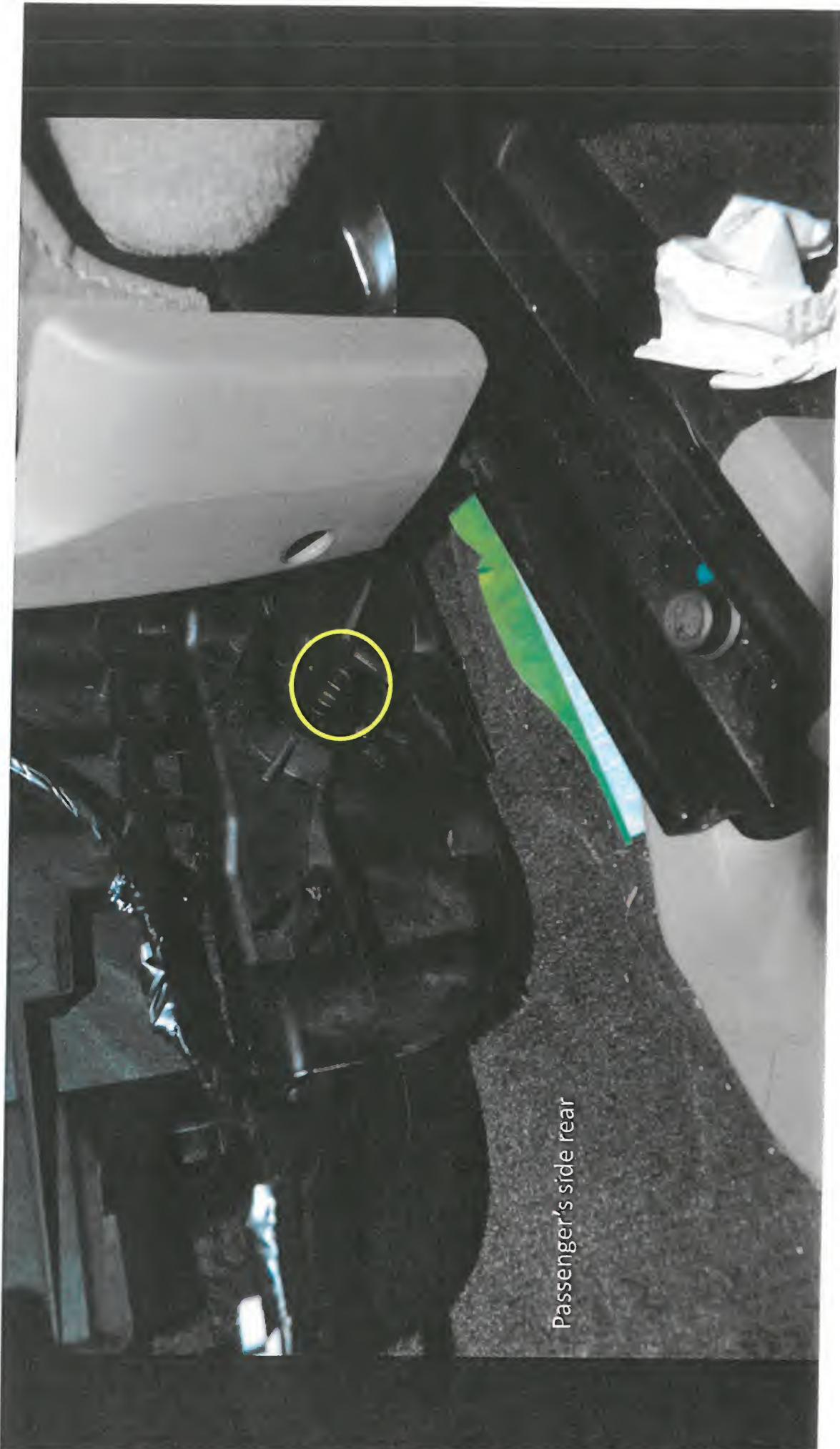




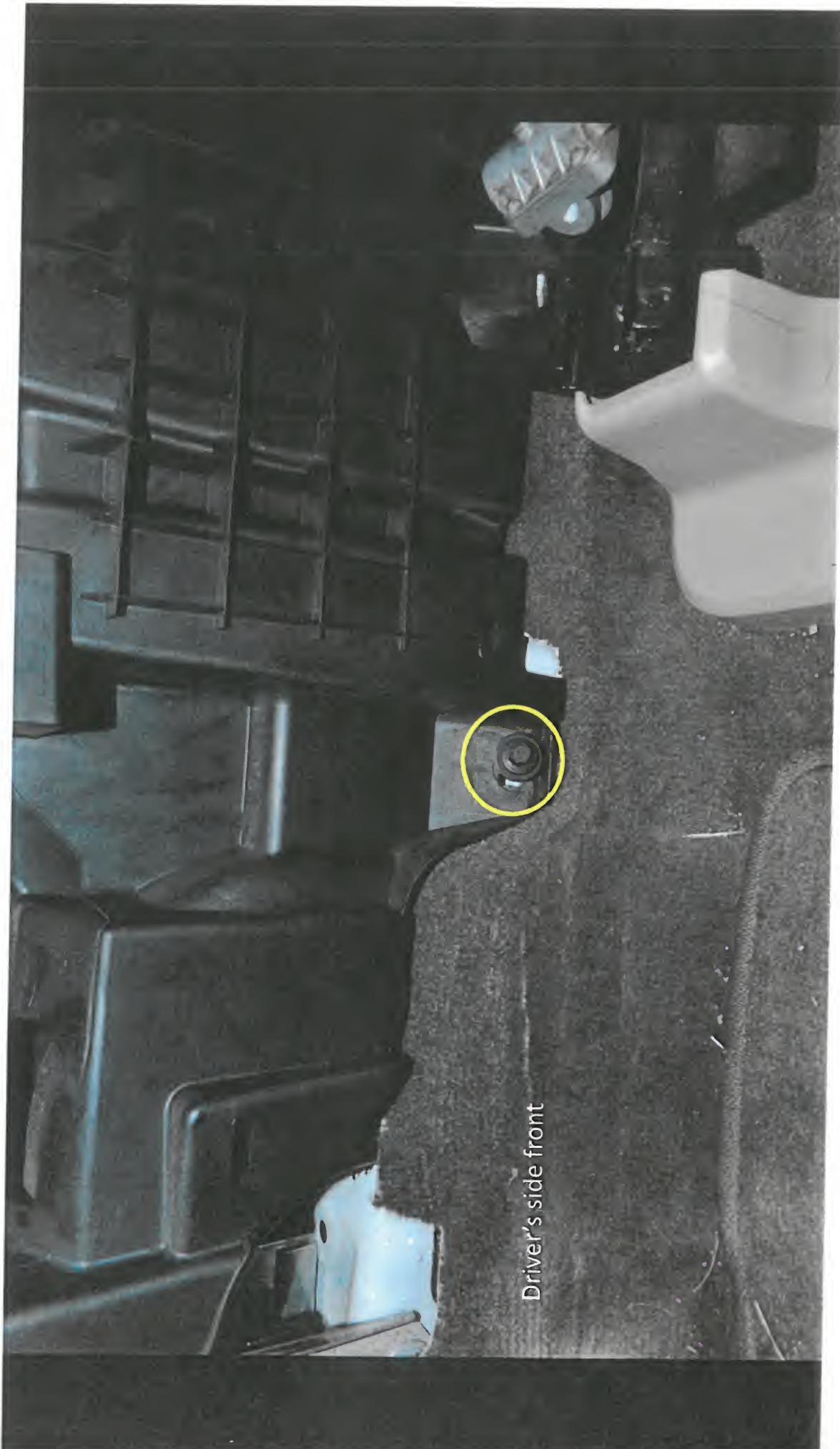
Passenger's side front



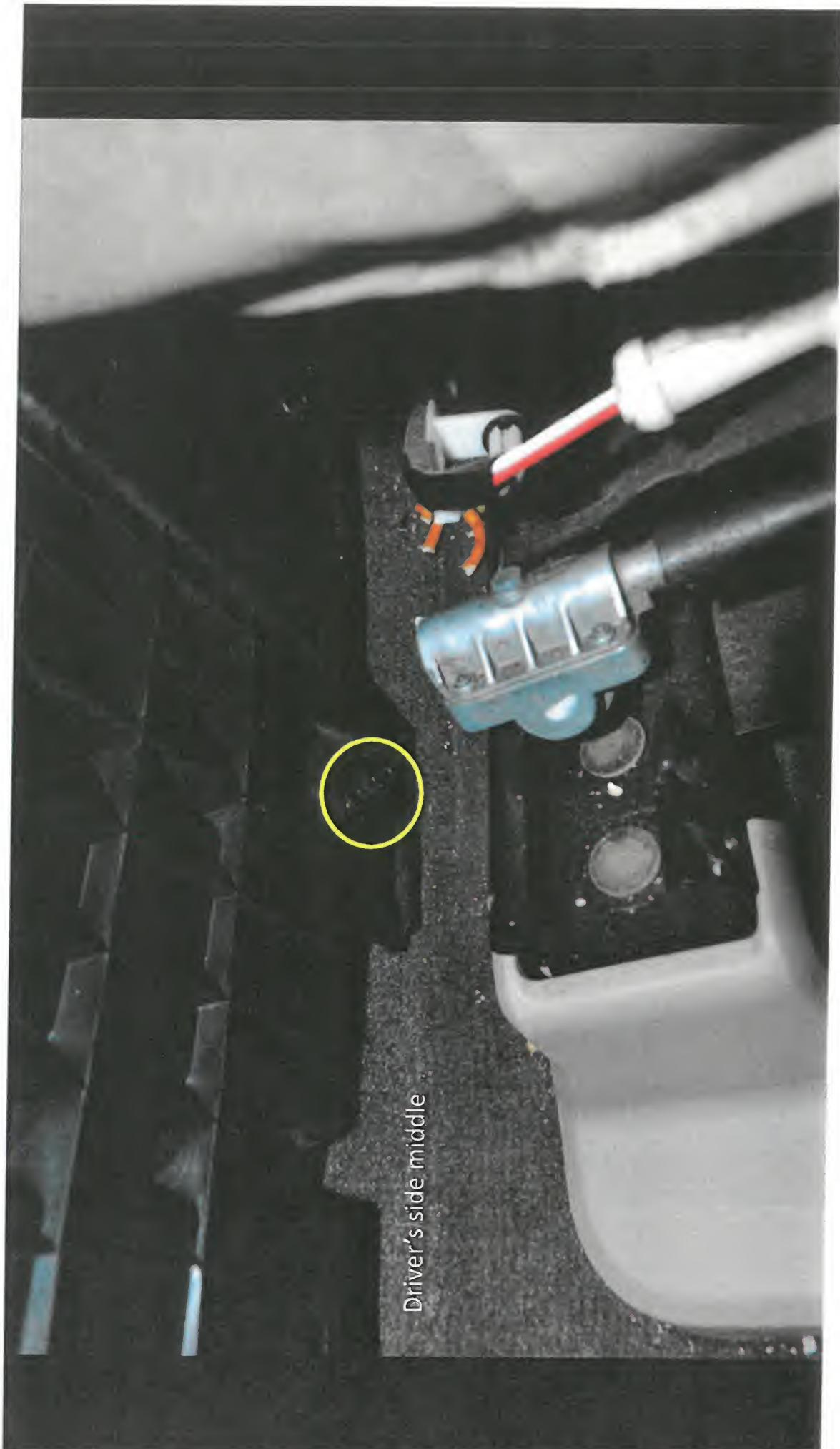
Passenger's side middle

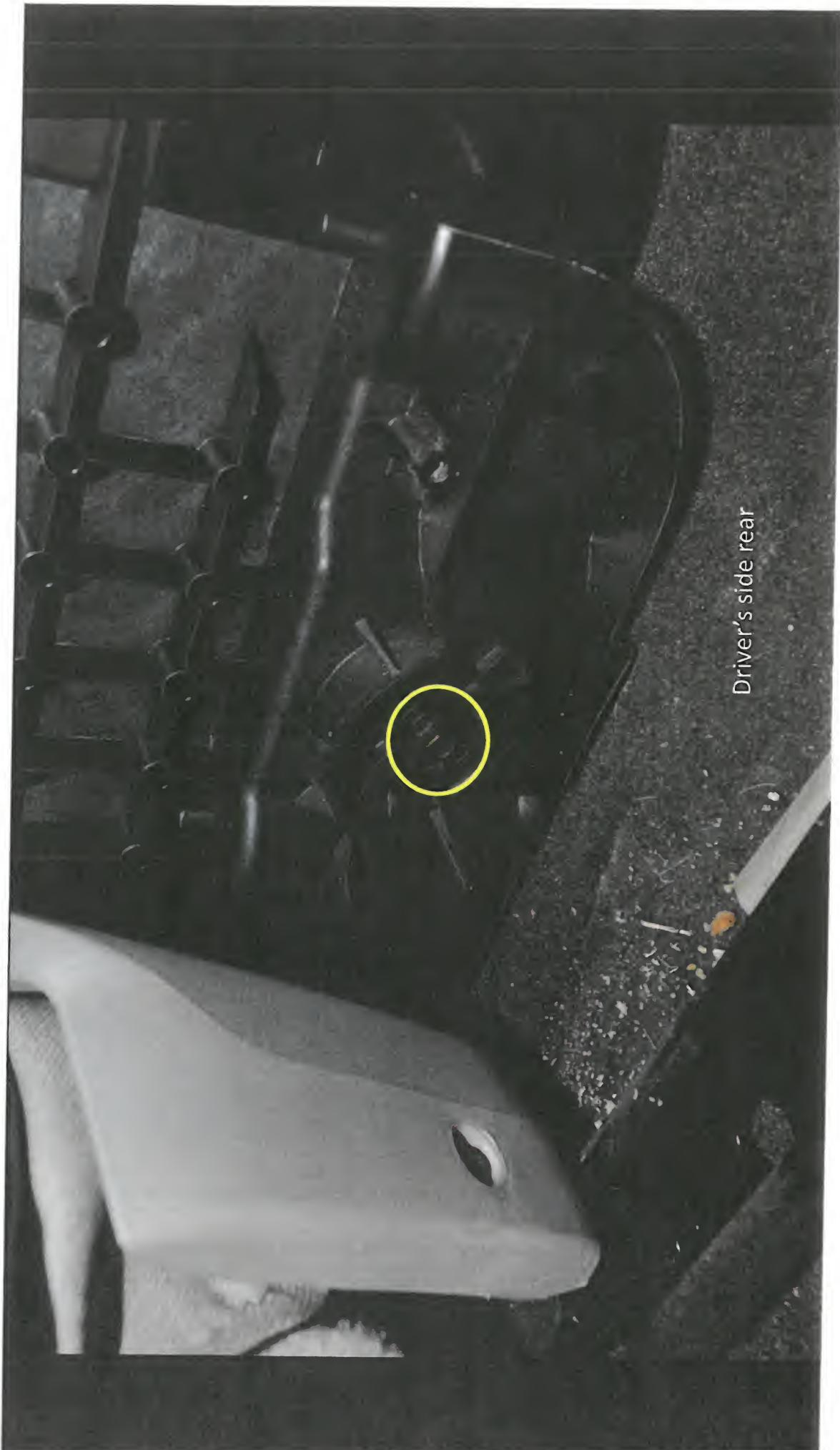


Passenger's side rear

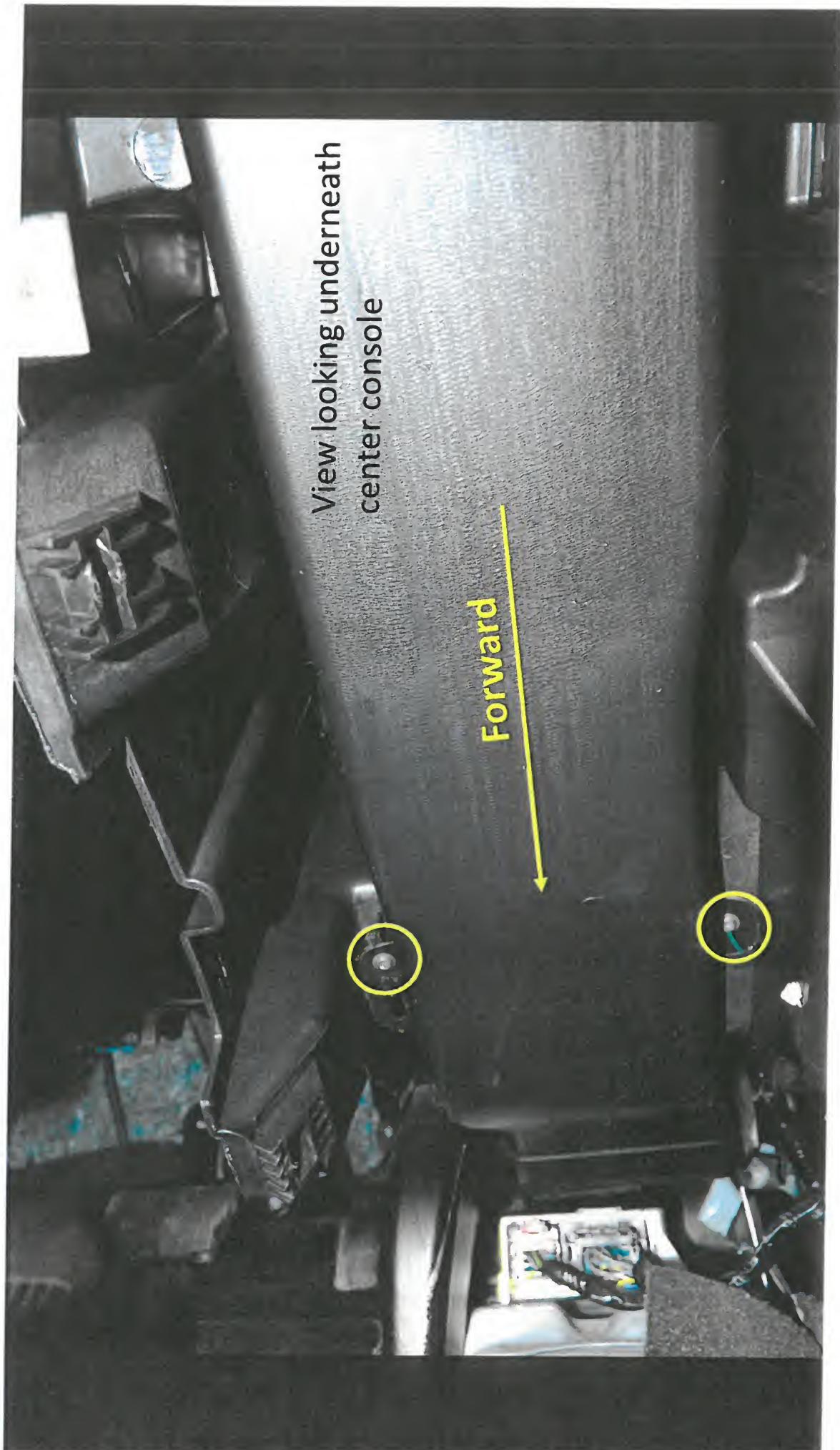


Driver's side front



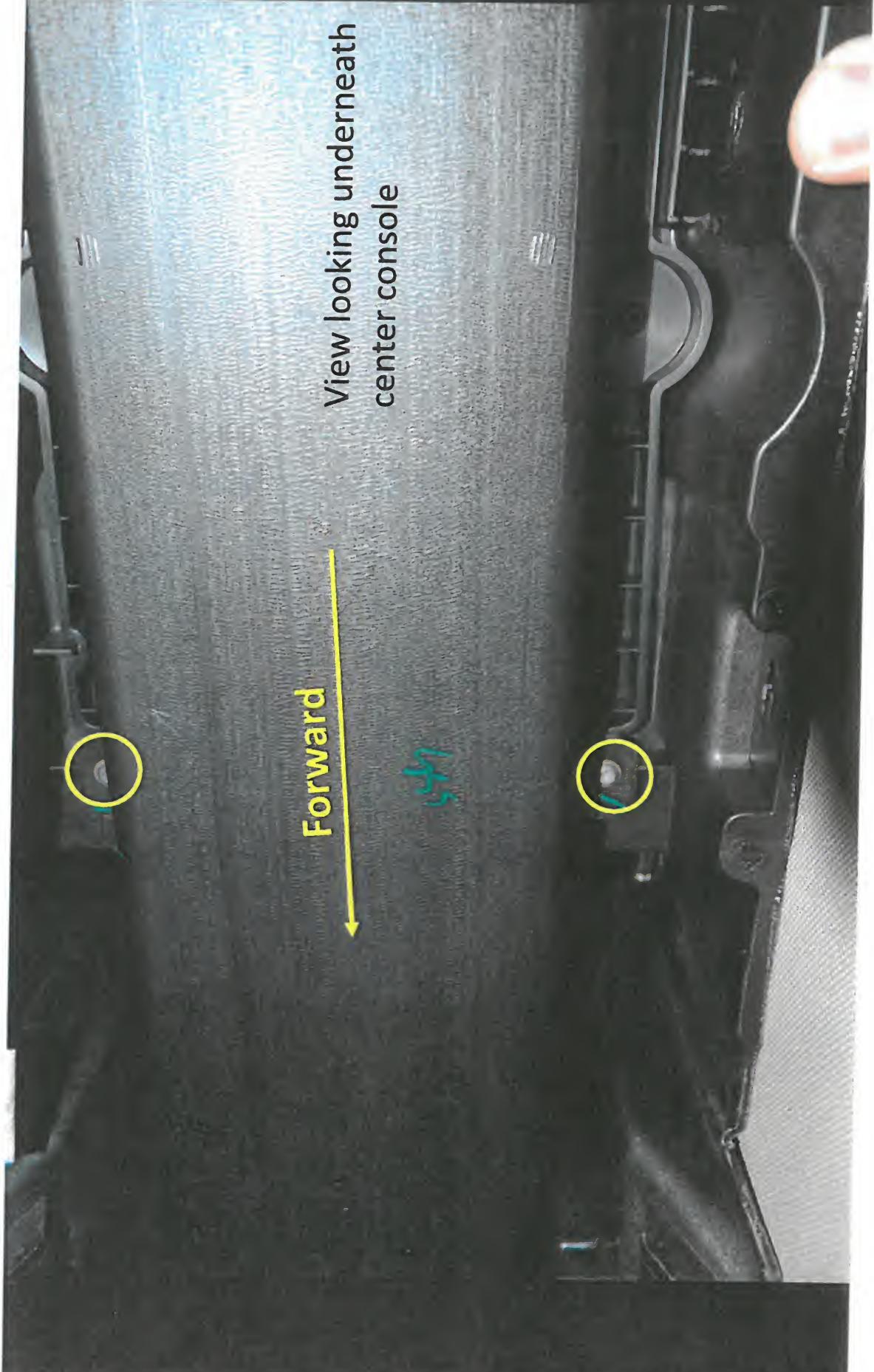


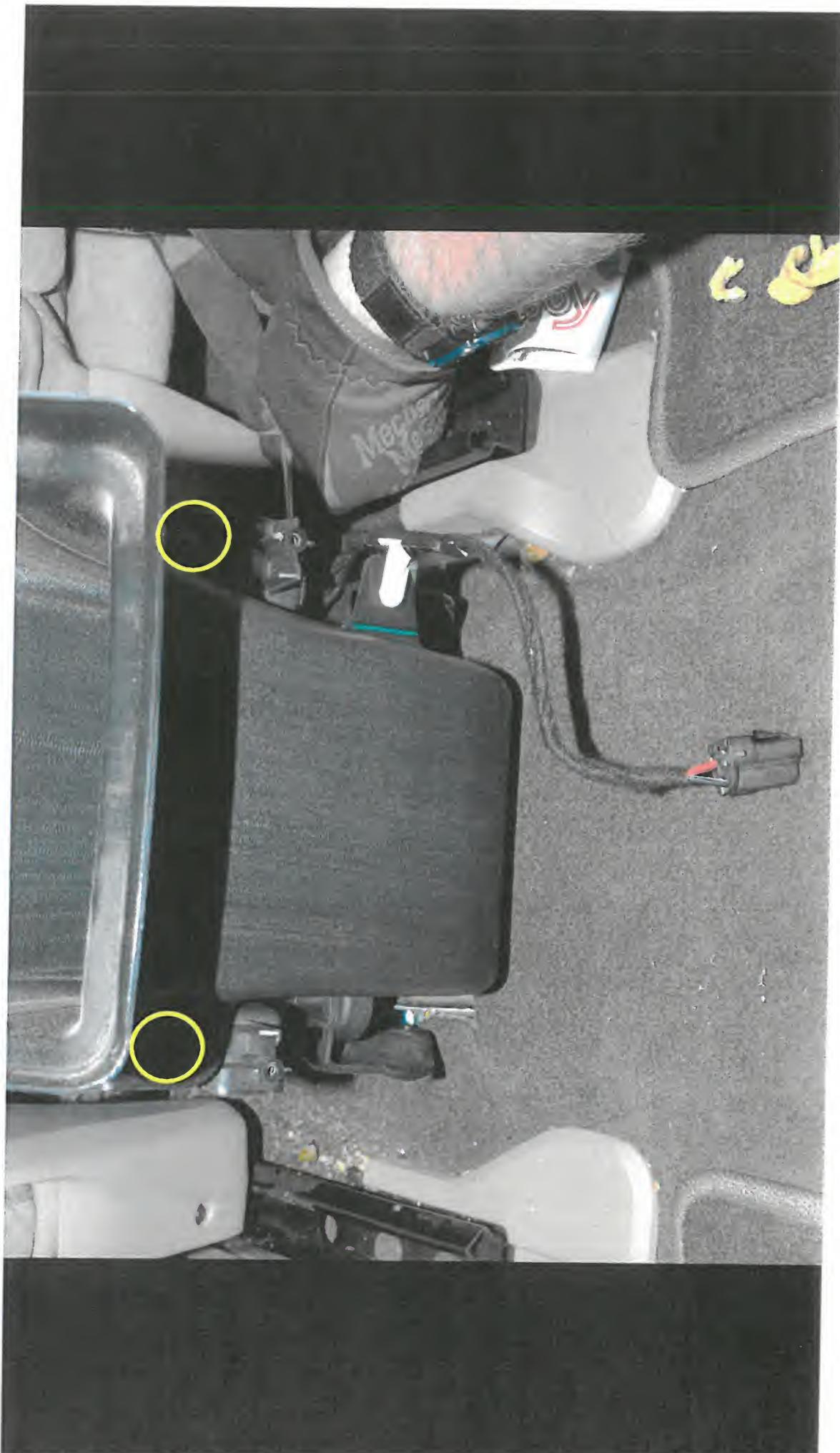
Driver's side rear



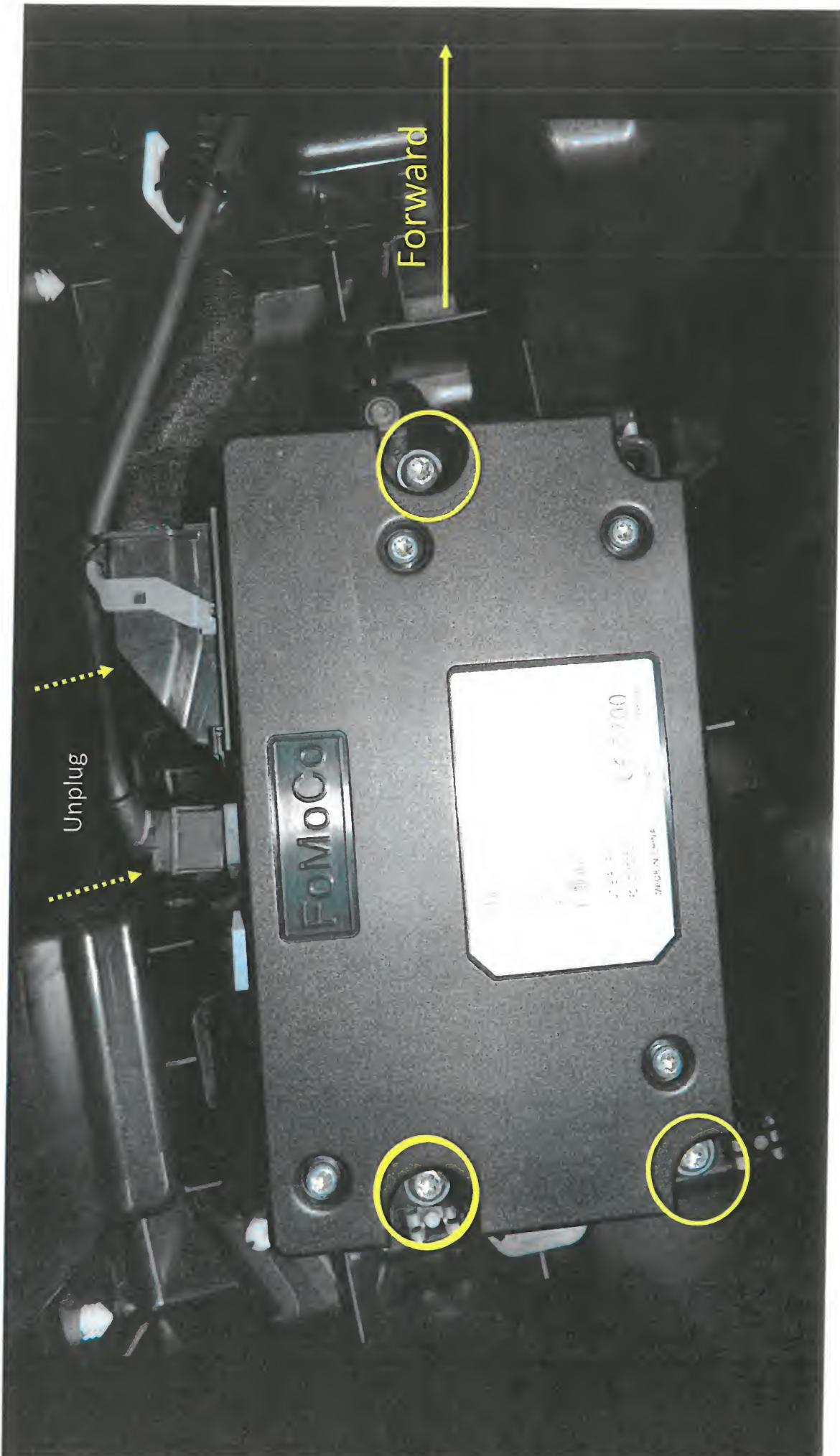
View looking underneath
center console

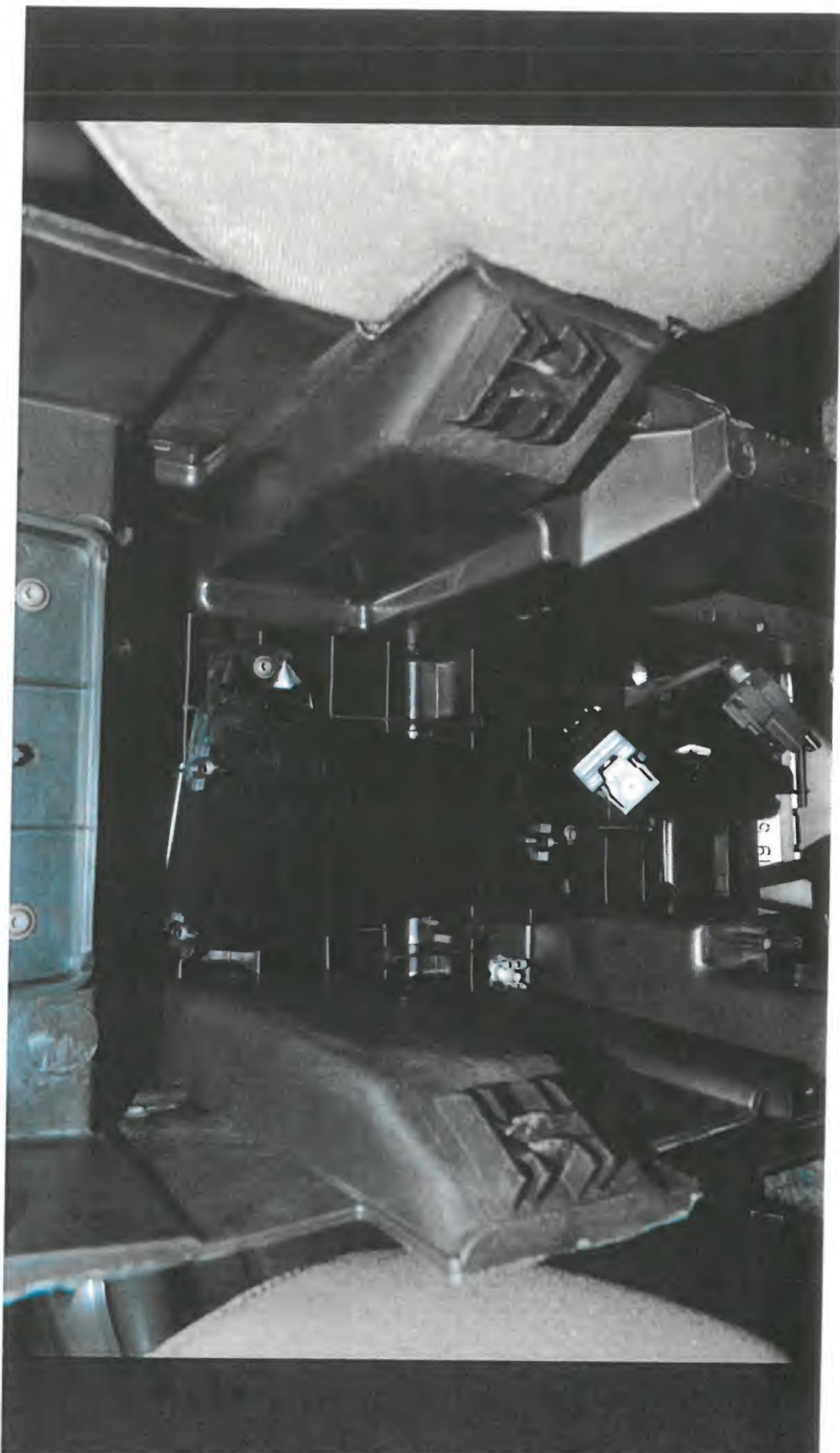
Forward















PARS: 0857-140213
BT ADDR: 00 21 00 30 70 26
BT QDC: 0214073
SN: CPAR0498

COFETEL RCPFOSY11-032 IC5248B-SSG1

FCC ID WDGGSG1

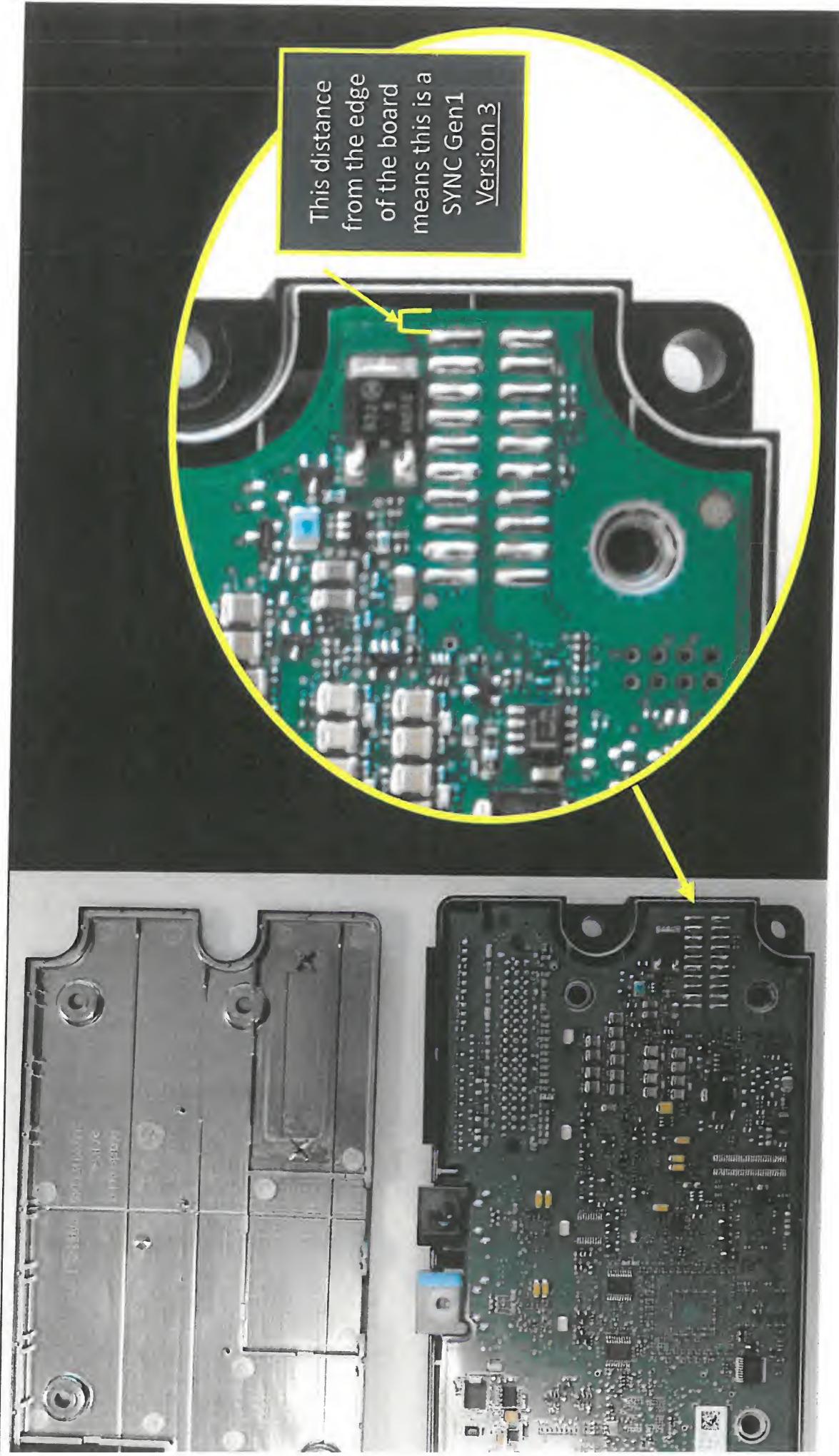
CE 0700

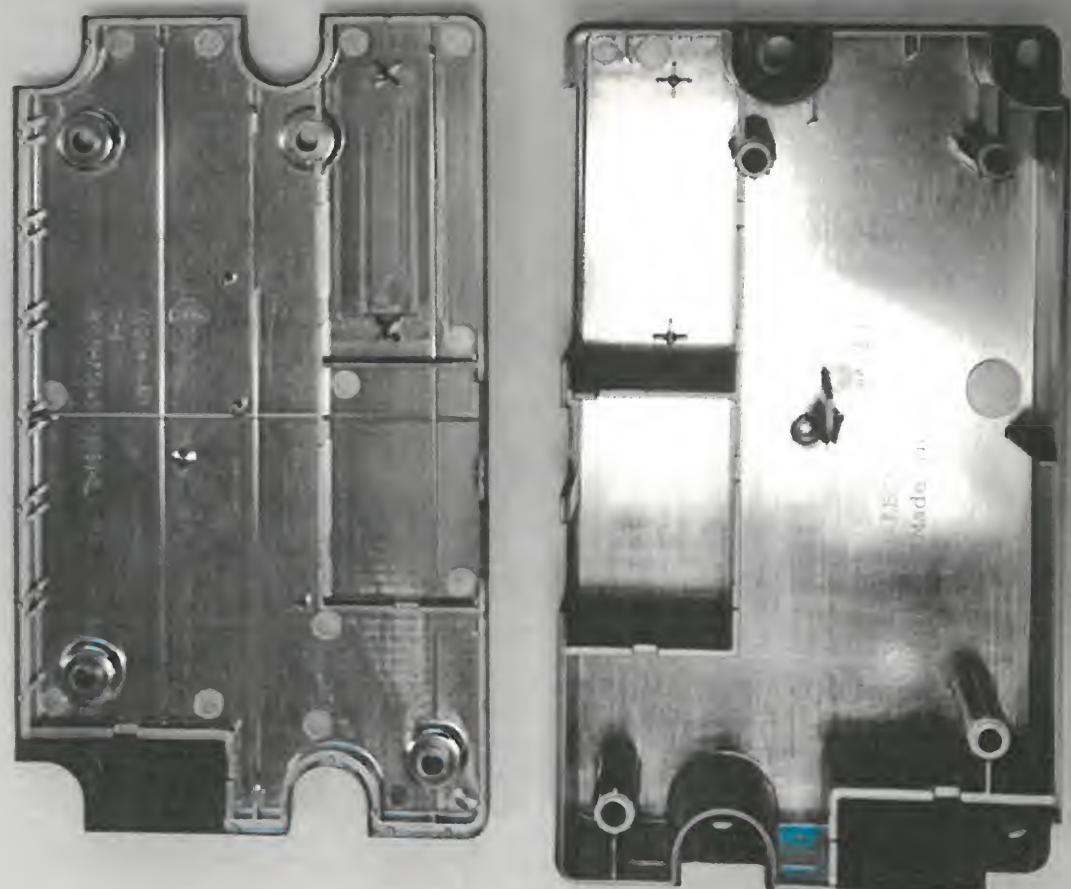
MADE IN CHINA

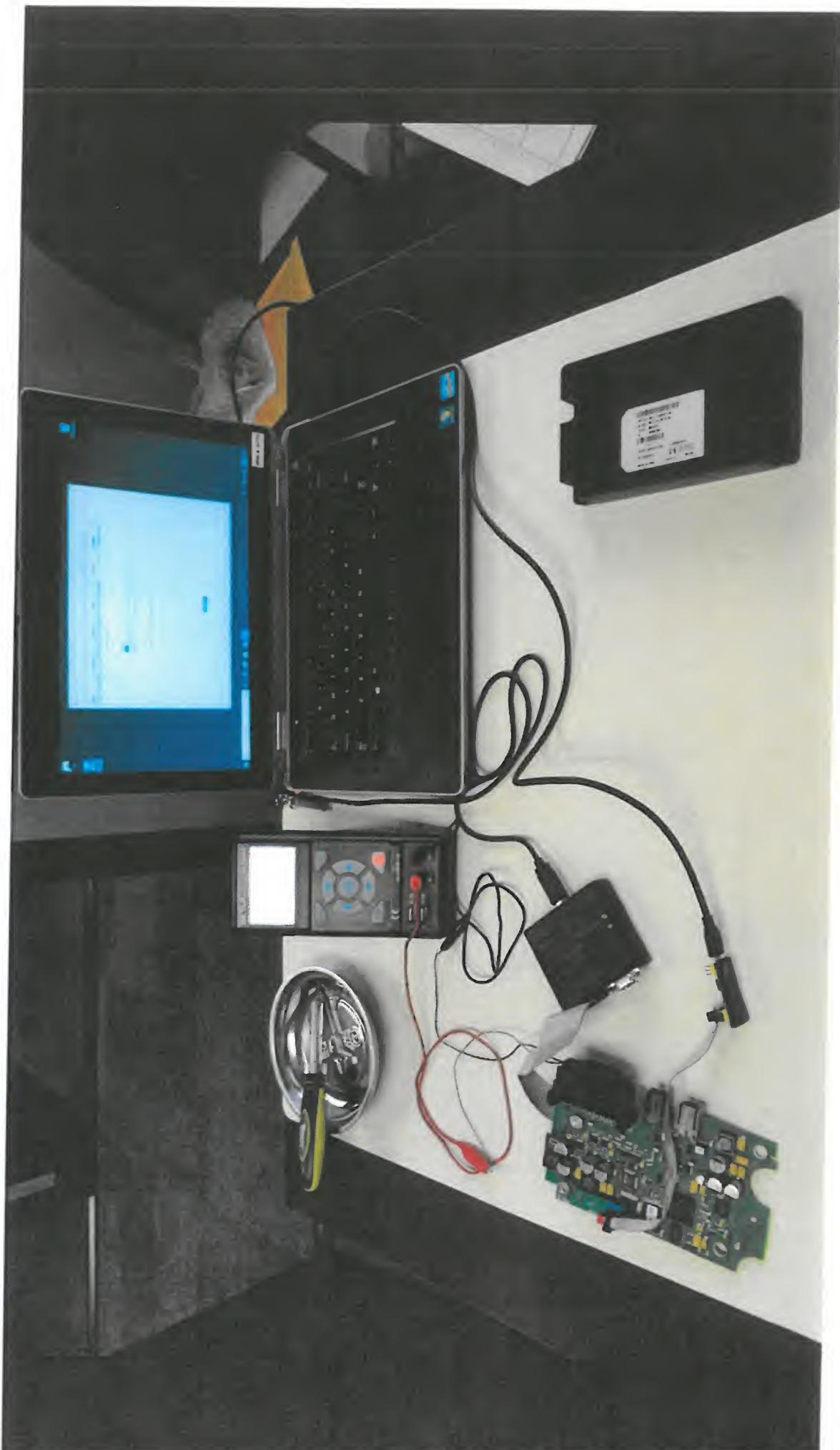
GJ1A 20121024

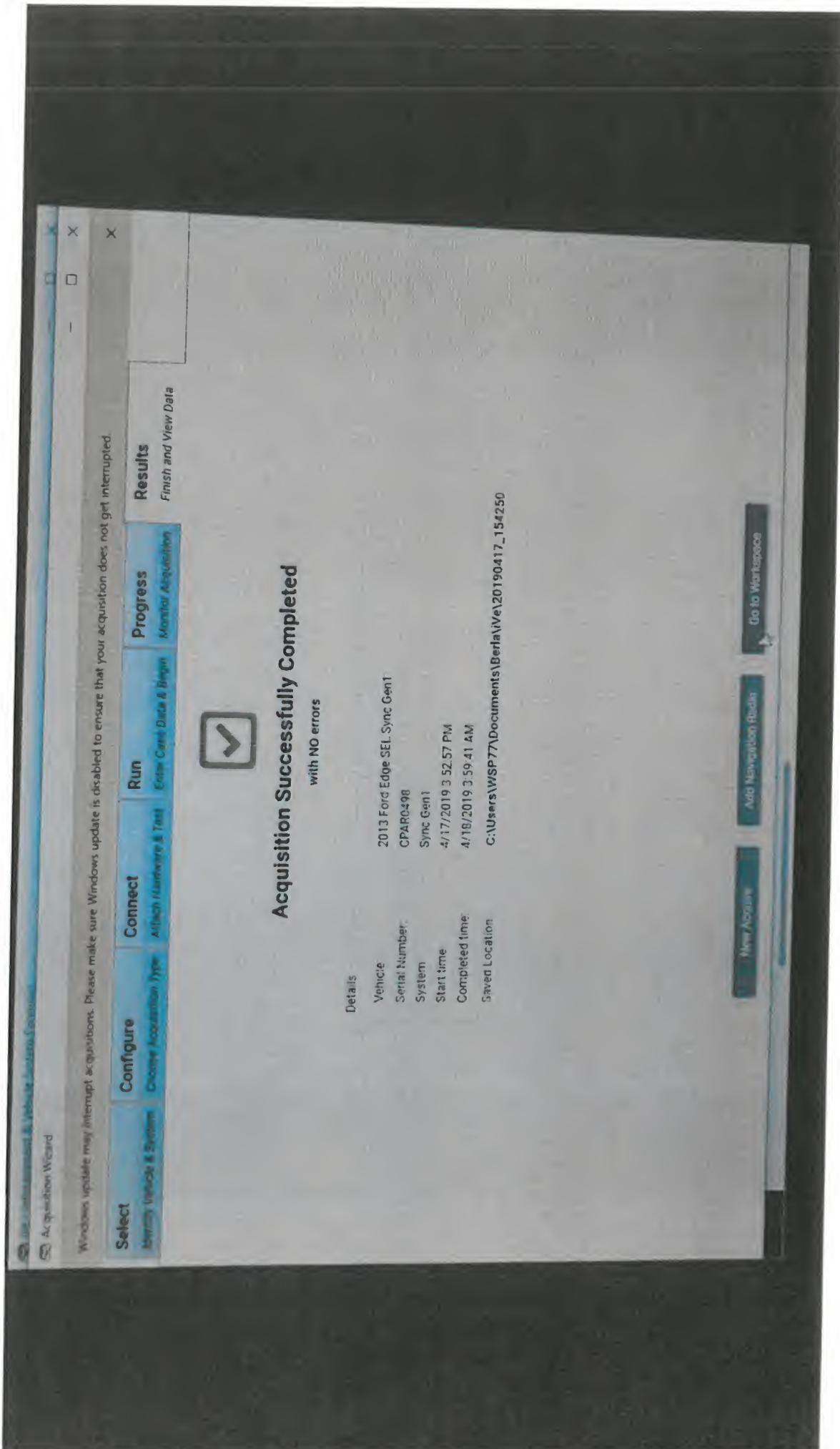
306

This distance
from the edge
of the board
means this is a
SYNC Gen1
Version 3









WASHINGTON STATE PATROL
CRIMINAL INVESTIGATION DIVISION

Investigative Report



FILE TITLE	DETECTIVE	CASE NUMBER
BERLA imaging assist	Benjamin J. McBride	04-19-009175
SUBJECT		OTHER CASE NUMBER
Bolton, James		SCSO# 1903342

Synopsis:

Stevens County Sheriff's Office (SCSO) was investigating a criminal case involving assault, threats, and extortion. They requested the assistance from the Washington State Patrol (WSP) with imaging the data from the infotainment system equipped in the suspect's vehicle. WSP Detective Larry McGill (770), a trained and certified Berla iVe infotainment system technician and analyst, agreed to help.

Details:

McGill, a member of the WSP Criminal Investigation Unit (CIU) based in Spokane, asked if I, Detective Ben McBride (1135), was available to assist him with accessing an infotainment module in a 2013 Ford Edge for SCSO Detective Travis Frizzell. After obtaining permission from my supervisor, Sergeant Jason Kraus (178), I told McGill I would be able to assist.

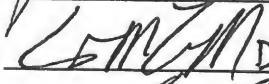
As planned, McGill and I met at the north office in Spokane on Wednesday, April 17, 2019. Sergeant Scott Davis (137) also met with us. After a brief meeting, the three of us drove to the SCSO office in Colville to meet with Frizzell. We arrived at the SCSO office at 9:02 a.m.

Frizzell briefed us on the basics of this case and showed a signed search warrant to McGill regarding electronic data from the involved vehicle's infotainment system. After this meeting, we left the office and traveled to their evidence facility in the 100 block of Degrief Road in Colville. We arrived at 9:33 a.m.

Frizzell provided us access to the facility and there was a white 2013 Ford Edge (WA license BDE3849) stored inside. This vehicle was the one listed in the warrant. At 9:38 a.m., the vehicle was opened, granting us access to the inside. McGill prepared the needed equipment and tools and began dismantling the center console at 9:45 a.m. Under McGill's guidance, I assisted in dismantling the center console to access the proper module. McGill used the instructions provided by Berla, but did not locate the module in the listed area, behind the center console. After a phone call to Berla help support, McGill advised the module was underneath the center console and the entire console would need to be removed. He also received an email with instructions to remove the console in a similar vehicle. McGill and I removed the console and located the module at 11:30 a.m. McGill

Page 1 of 2

Officer's Signature  Date 4-29-19

Peer Reviewer's Signature  Date 4-29-19

Supervisor's Signature  Date 4-29-19

photographed this process. McGill removed the module from the vehicle at 11:37 and provided it to Frizzell. After he logged it as evidence, McGill took possession of it for imaging.

During the earlier meeting, Frizzell mentioned there may be dye powder in the vehicle which would turn purple when wet. He advised he would be looking for evidence of this in the vehicle. While we removed the console, I observed many places in the vehicle which appeared to have this purple dye. There was a service reminder tag on the floor, between the driver's seat and console, which had this dye on it. There was dye on various parts of the center console, seats, floor, and door seals. Frizzell documented this evidence.

We cleared the evidence facility at 11:50 a.m. and returned to Spokane.

On April 18, 2019, McGill advised me the imaging was complete and he would return to Colville to install the module back into the vehicle. As removal was a lengthy process, I agreed to go and assist in the installation. McGill and I left Spokane and arrived at the SCSO office at 10:20 a.m. McGill provided Frizzell with a disk containing the recovered data and then we went to the evidence facility, arriving at 10:53 a.m.

McGill and I worked together to install the module and center console back into the vehicle. During installation, McGill continued to photograph each step for future use in creating instructions for console removal on this vehicle. We completed the installation at 12:31 p.m. and cleared the facility at 12:49 p.m. McGill and I returned to Spokane.

End of Report.